

Hybrid War: High-tech, Information and Cyber Conflicts

Yuriy Danyk; Tamara Maliarchuk; Chad Briggs

Abstract:

This article examines the advanced technological, information and cyber components of hybrid war and the introduction of suggested countermeasures to counter information and cyber threats and attacks. The main hypothesis of the authors is that revolutionary development and rapid implementation of technologies in innovative ways in all spheres of life facilitate and shape the basis for the transformation of theoretical and practical paradigms of war and conflict. The focus of the article is on the hybrid nature of modern conflict.

Introduction

Analyses of geopolitical and geostrategic environments have hinted at a reformulation of both the philosophy and art of war, developments brought about from the deployment of new technologies that allow variable intensity and strategies in conflict. These new methods, when combined with traditional understandings of conflict and security, are often coined as “hybrid” warfare. This paper examines the nature of hybrid warfare in Eastern Europe, with a specific focus on the tactics and strategies employed by Russian and allied forces in Ukraine since 2014.

The concept of hybrid warfare is not particularly new, representing a combination of conventional and unconventional/irregular warfare, extending beyond the battlefield to encompass economic, diplomatic, information (including psychological, cyber and misinformation), and political warfare.^[1] The concept is primarily based on the ability to target distant objects and processes through non-traditional military means, particularly those critical to state and military functions. As an asymmetric approach, hybrid warfare attempts to achieve large-scale consequences utilizing modest means, such as inhibiting an adversary’s military operations or preventing popular political support.^[2] Overall, hybrid conflicts coordinate so-called soft actions employing a more holistic strategy that varies in intensity at different stages (initiation, acute phase, solution), which seek to destabilize internal and external processes of a state. An overall objective is to disrupt the targeted state by encouraging the destabilization of the economy, frustration and disaffection of the population, splintering of minorities or aggrieved populations, creation of conditions encouraging controlled and uncontrolled migration, suppression of civil resistance, and disruption of critical infrastructure. It is aided by the selective application of intelligence capabilities, special forces’ operations, conventional military forces, and irregular combatants (terrorists, criminals, militia groups, mercenaries, resistance movements, guerrillas, etc.). A contemporary example of a hybrid conflict can be clearly illustrated by ongoing and recent combat actions occurring in Ukraine,^[3] Georgia,^[4] and, more recently, in specific European Union countries.^[5]

The concepts presented here differ slightly from some portrayals of hybrid warfare in the West (West, Western World or Western Civilization are countries in Europe, North America, Australia, Israel, Japan, South Korea, etc., united by the common views and perception of some unity on key cultural, political and economic signs, highlighting them on the background of other countries,^[6] which focus on the so-called ‘Gerasimov doctrine’ of *maskirovka*, of operating below the threshold of open, conventional warfare while maintaining plausible deniability of involvement.^[7] In contrast, this paper describes some of the tactics deployed in support of forces often (but not always) operating in a conventional manner, which are enhanced through the use of new technologies that afford greater penetration of asymmetric actions into critical elements and vital systems of the opponent. In other words, critical elements of a system are significant key elements (components, subsystems) of different systems (referring to fissures, weak points in a system).^[8] Pressure on these weaknesses can lead to a cascading, synergetic, destructive systemic change (violations) of critical components and related systems.^[9]

Application of hybrid warfare looks for more than critical vulnerabilities in hardware such as communications, infrastructure, or transport. Increasingly, actors such as Russia and ISIS have attacked

vulnerable points in ideologies and institutions, as well as taking advantage of social discontent or perceptions of corruption to level the conflict playing field.[10] These larger strategic fissures have allowed greater success for those undertaking information or asymmetric warfare against the West. The dominance of neoliberal ideas led to an increasing gap between rich and poor, and increased pressure of the middle class. As a result, there are fundamental changes in the economy, sociopolitical and psychological situation and reassessment of the core values, the growth of populism in many countries around the world. The Brexit vote in the UK in 2016 and the election of Donald Trump to the US presidency are reflective of this anxiety with socioeconomic conditions, calling into question decades-old institutions such as the European Union and NATO.[11]

Preserving competitiveness and leading roles on the world stage requires appropriate economic power and a high level of education and science development, resources available mainly for centers of world power. Countries, lacking such access, may feel left behind, and the loss of opportunities and the rate of high-tech development in economic and defense sectors inevitably leads to the loss of their leading position and the redistribution of spheres of influence among more powerful actors. Striving to take control over competing “centers of world power” and to obtain unhindered access to strategic resources or, in contrary, to prevent such development of a situation, leads to violation or absorption of their security zones and spheres of influence. As a result, there is a dangerous mutual rapprochement of centers of world power with inevitable conflict of interests.

These conflicts are defined in Huntington-type civilizational clashes, with people’s cultural and religious identities as the primary source of conflict in the post-Cold War world. American political scientist Samuel Huntington argued that future wars would be fought not between countries, but between cultures.[12] Clashes can also be Machiavellian attempts at undermining strategic adversaries, and leaders will often perceive a need to develop military power projection, that does not result in the *ultima ratio regum* [13] decisions, where violent conflict results in destruction for both sides. Instead, there is a necessity for new tools to achieve goals without direct and visible aggression.

The desire was for technologies that could provide not only new power of armaments, but also the ability to exploit weak points in all spheres of functioning of a state. In contrast to information campaigns of the past, new technologies allow the possibility to achieve strategic goals by unconventional and cognitive effects (technologies of social influence and manipulation, cyber sphere, information weapon, possibilities of significant damage of control systems of a state). Technologies, such as social media, made it possible for an actor to remotely influence all main institutions and infrastructure of a state. It formed a basis for unconventional invasions of territory, often even without the use of the conventional military components. Or its presence made possible externally organized and supported resistance movements and terrorism, which could also achieve strategic goals of uncertainty and institutional damage without violence.[14]

Thus, the “hybrid war” is a high-tech conflict. It is a continuation of the policy of a state and/or coalitions, political groups, transnational corporations, and non-state actors. The purpose of the conflict is to impose an actor’s will on their opponents through integrated adaptive and asymmetric synchronized destructive effects on them in a multidimensional space and in various spheres of life. Hybrid war is rationally combined with conventional and unconventional components, an emphasis on multiple sources and modes of attack, synergy of results and a high level of uncertainty for opponents of what final strategic goals may be.

In hybrid conflicts the main goals are taking control over society, influencing the mindsets of people, and manipulating people, who are responsible for making important decisions in a state. The enemy aims to manipulate core values, motivational factors and cultural basis, and the strategic, communicational and critical infrastructure of a country. This is achieved by complex, balanced realization of effects with the use of soft and hard power. That’s why critical elements of systems, in other words, objects for asymmetric actions in hybrid conflicts, are significant for a system key element (components, subsystems) of state, political, diplomatic, social, technical, sociotechnical, energetic, financial, cyber, socio-cyber, information and other systems. The influence on them in the limits of optimal measures and correlations of space parameters, time and resources for the influencing party leads to desirable, goal-directed, fast, cascading, synergistic and destructive for system changes (violations) in their relations, structures, processes and results of functioning.

Hybrid War in Ukraine

One of the distinctive features of the “hybrid war” in Ukraine is how much it has occupied all aspects of social life, how wide-ranging, multidimensional and employing multifactorial information focused on both psychological and cyber sources. A good example of such activities is provided by the innovative and highly technical samples of weaponry and military hardware applied during the 2014 Crimea annexation, as well as the combat actions in the east of Ukraine [\[15\]](#) since 2014:

- Electronic warfare systems and complexes and other types of electronic countermeasures;
- Modern information and communications systems;
- Innovative weapon control systems;
- Integrated reconnaissance-strike complexes;
- Innovative, including automated, software;
- Complexes for conducting information-psychological activities and actions in cyber space;
- Environmental control and space systems;
- Robotic systems (especially unmanned aircraft complexes) and countermeasures.

The technology did not exist on its own, but was a part of a larger and strategically designed campaign to undermine confidence in central institutions. The initial goal was to establish a general loss of civic confidence in the government of Ukraine by launching an information warfare campaign aimed at discrediting government authorities, Ukrainian Armed Forces authorities, and encouraging an increase in crime and separatism activities. This information campaign fostered socio-political destabilization in the country and continues to negatively affect the country. [\[16\]](#)

This strategy successfully integrated innovative cyber technologies in coordination with carefully planned unconventional and irregular forces on the ground, leading to the 2014 annexation of Crimea and the military conflict in South-Eastern Ukraine. In response to both unconventional and conventional security threats, as mentioned above, most countries with rapid response capabilities focus on two primary components to their security apparatus:

- Deterrence potential, consisting of traditional branches of the armed forces (land forces, air forces, navy);
- Innovative warfare potential. The potential consists of military equipment and personnel of Special Operations forces, information-psychological operations and electronic warfare, as well as cyber forces (cyber intelligence, security and operations), branches of intelligence (electronic warfare, open-source intelligence (OSINT), technical types of intelligence, surveillance, and reconnaissance (ISR), etc.), operational control communication, military units, which are equipped with robotic (unmanned aircraft) complexes and countermeasures to associated attacks, other highly technological resources and measures. [\[17\]](#)

Generation of Highly Technological Warfare

Technological progress has always been a driving force behind military strategy. Technologically intensive wars are connected with design and wide use of advanced technical tools, and systems and complexes created by the most developed countries. These developments give certain countries a distinct advantage during combat actions without the necessity of massing overwhelming conventional forces. However, more technologically advanced states may be more vulnerable to certain attacks. [\[18\]](#)



Photo 1: Application of innovative constructions of Jam-Proof Robotic Complexes by military personnel of S. Korolov Zhytomyr Military Institute.

New opportunities for targeting vulnerabilities, combined with new weapons and military equipment, led to the development, implementation and practical use in leading countries of new strategic concepts of warfighting: “Global Warfighting,” “Global Visibility,” “Global Coverage,” “Net Centric Warfare,” “Hybrid Wars,” “Strategic Paralysis,” “Parallel Wars,” “Controlled Chaos” wars, “Unlimited Wars,” “Controlled Wars,” etc. These advanced concepts consider the combat effects on potential enemies from a distance via the use of intelligence information support, information and precision weaponry, robotic technologies, and other means. Innovative control technologies, as opposed to combat actions, allow attacks to be conducted primarily against priority targets with the maximum speed and precision of actions affecting “critical” components, over any territory of a state (region) without any physical presence required. The realization of such force projection allows the attainment of strategic objectives without the historic obstacles to victory of time, distance and intense manpower logistics. As long as the object of a security strategy is destabilization of one’s opponent and exploitation of weaknesses in critical nodes (subsystems, components, objects), then it is not necessary to control territory by force. Rather, these vulnerabilities of security leakages, weak logistical links, security gaps, allow the disruption of essential systems necessary to continue or even initiate the fight. The dysfunction of the system or any other destructive impact on the target inhibits a state that has not been able to take preventative measures to use its capability to respond adequately to subsequent warfare and warfighting.

In essence, state defense support, under conditions of hybrid threats and hybrid warfighting, demands the existence of a balanced and full-spectrum national security and defense sector. The armed forces remain the key component of national security, which must respond to modern and future challenges and threats. Armed forces should be equipped with supplies of advanced weapons and military equipment, relevant organization, and units staffed with skilled personnel. Skilled personnel should be able to conduct powerful information and special operations with the purpose of influencing economics, politics, energy systems, information and communications, command and control, local and enemy populations.

Military Components of Hybrid War

The peculiarities of the military component of highly technological and hybrid wars include:

- The transition from strategic control to operational combat control, the basis of which is real-time battlefield management and informational superiority over enemy actions: intelligence, decision-making and implementation, impacts (deprivation) [19]
- The transition of the primary warfighting responsibilities to cyber and airspace environments, including ISR [20]
- Warfighting means increasing based on robotization, stealth concepts, and warfighting from a distance
- The formation and use of situational and automated surveillance and attack complexes and systems
- Wide use of effective non-lethal weapons [21]
- The increasing use of irregular militia groups (paramilitary forces) [22]
- Related increase in asymmetric combat actions
- The increasing role and widening of Special Forces involvement [23]
- The increasing reliance upon and use of radio-electronic, psychological and information warfare via cyber assets [24]
- The transition toward enemy-adapted warfare in all spheres of action.[25]

Information and Cyber Actions

A combination of research and combat analyses indicates that cyber-related actions and information warfare are increasing in both scope and importance for warfighters. In this context, hybrid warfare and the use of cyber assets as part of it is one of the most important factors for understanding the future arc of conflict. Combat actions in Illovoysk and Debalcevo in Ukraine were preceded by a significant burst of activity in information space. Negative information on key authorities of Armed Forces of Ukraine and government representatives was spread widely (usually outbursts of negative information in the Internet preceded the start of new combat campaign).[26] This is a common tactic, designated by Duggan as cyber aggression, coupled with disinformation from proxies and false fronts on the internet.[27]

Information and psychological operations (actions) of the enemy in cyber space require the use of different Internet resources. The examples of information and psychological operations are preparation and spreading of particular information in social nets and other Internet resources for discredit of Ukrainian authorities, ATO command and military personnel in the framework of campaigns “If not the Generals,” “Generals-Betrayers of Ukraine,” “Hail to the Ukrainian Artillery,” etc. Disinformation or unchecked, false information including the use of special technologies of promoting the rates of such messages through Internet are often spread in national cyber space as military patriotic resources. It is necessary to mention that some Internet resources are hosted by the Russian Federation in Moscow [28] (Photo 2).

The content analysis and modeling by Infostream concerning actions in Debalcevo in February 2015 illustrate fluctuations of the amplitude to a degree critical to the spread of messages.[29]


IP	93.170.76.83
Хост:	93.170.76.83
Город:	Moscow 🇷🇺
Страна:	 Russian Federation
IP диапазон:	93.170.76.0 - 93.170.76.255
Название провайдера:	PE Trofimec Dmitry Aleksandrovich
	подробнее

Photo 2. An example of Internet resource, discrediting Ukraine Armed Forces' authorities, hosted in the Russian Federation.

Media analysis has demonstrated the significant consequences of mass usage of widespread, negative social political information campaigns. First, cyber aggression against key figures in government is expected to encourage the widening range of negative information streams in order to aggravate existing civil mistrust and anti-government behavior. When this is extended into social media, the spread of false and malicious information encourages beliefs and behavior that would normally be kept in check by existing social mores and civic expectations. Even if information does not create a conscious change in beliefs, it can impact the interpretation of future information by providing effective anchoring and priming media.[30] This can aid a domestic aggressor wishing to influence the course of the conflict in order to weaken support for the target government. In some cases, such information warfare can replace kinetic operations, undermining defensive campaigns before they even need to begin.

Cyber aggression often conceals its actors and motives, shrouded by technological methods that can mask their manipulative goals. The methods of concealment include anonymous claims to authority, news items manipulated with half-truths, repetition of messages, information overload, cyber-pseudo operations (government posing as insurgents), sock-puppeting (government agents playing the role of online commentators), and astro-turfing (creating of false grassroots movements).[31]

In Ukraine, the consequences of such actions since 2014 have resulted in discrediting the Armed Forces, disaffection and mistrust directed toward the primary military and political authorities of the state, sowing of doubt concerning the necessity of military actions, and damage to civic morale and the encouragement of desertion among military personnel. In the absence of specific countermeasures against discrediting the Ukraine Armed Forces, disaffection and mistrust, one can expect as a result weakening of state and military capabilities needed to respond to aggression. Moreover, the actions of national media outlets, whether intentionally or not, organized by the Russian Federation, aggravated an already complex situation by appeals to encourage simple narratives. Media reliance upon untrustworthy or false sources, negatively-framed news stories, and criticism of the actions of Armed Forces' authorities contributed to the information campaign of the enemy.[32] Russian forces were able to exploit preexisting vulnerabilities in social, political, and economic systems leading up to open conflict, with the height of such operations coinciding with the onset of kinetic operations in Donbas in 2014. The use of cyber assets has been a form of force projection that helps initiate crises far ahead of and beyond the frontlines, creating forms of more complex crises that affect energy infrastructure, banking systems, and political leadership, and not solely the armed forces fighting on the frontlines. Again, the extension of traditional military conflict is not a new strategy, but new technologies have been able to provide both the means and vulnerabilities to allow such operations at a scale not often witnessed before, and with a smaller investment in resources on the part of the aggressor.



Photo 3. The example of reputation manipulation of Armed Forces authorities by mass media.[33]

The effective prevention and detection of enemy’s information and psychological actions in cyber space and our quick reaction require the creation of national centers of countermeasures to information and cyberattacks. The national centers should unite and facilitate coordination among international centers providing countermeasures to cyber threats. The national centers should provide monitoring and detection of destructive effects and identify signs, mechanisms (strategies, tactics, techniques, forms and methods) of their implementation. They should detect the sources and variants of spreading dangerous contents, interconnection during the operation (actions) among various Internet resources for defining the aim of the actions and possible results.

Measures for neutralization of destructive information and cyber effects and their sources are:

- Warning the owners (if they are known) of Internet resources about restrictions against spreading fake, untruthful information with the recommendation of its deletion if the information harms subjects and objects of national security (person, society, state)
- Creating public registries for unreliable/suspected resources.

In cases when it is impossible to define the owner or moderator, and the content may turn into a real threat to subjects and objects of national security, it is recommended to block electronic information resources, delete the content, etc.

Crisis Situations

Crisis situations appear as external forces (aggression and/or natural) exploit vulnerabilities and overwhelm critical systems in a target region or force. These crises can appear as a result of information and cyber actions in conditions of hybrid conflict, as a realization of information, psychological, and cyber threats (e.g. terror, economic, military, diplomatic, politics, etc.) directed against critical infrastructures of a state or military force’s command and control systems. This loss or intensive degradation of operability can be operationalized as a non-linear function, meaning that impacts may not be evident until the complete failure of the target system.

Effective countermeasures to crisis situations in cyber space according to ATO (the operation in occupied areas of Ukraine) experience can be realized in:

- Systematic development of forms, methods and means of operational detecting, protection and active countermeasures to information threats in cyber space
- Scientific research and development of specialized software and hardware capability for information activity in cyber space
- Professional military education and training based on combat experience and lessons learned in this sphere
- Conducting applied national and international training, war gaming and consultations
- Improving the training and education of military and civil specialists in the sphere of information and cyber security
- Operational implementation of lessons learned in national and international security systems.

Experience demonstrates that effective use of hybrid warfare methods results in largely unpredictable patterns of crisis and response. It is unusual for hybrid warfare practitioners to have clearly defined outcomes and event pathways, so likewise those responding to such strategies must be able to adapt in dynamic and rapidly shifting environments.

Technological design of well-known countermeasure systems in crisis situations, forms, methods and use of the systems must be oriented toward the formation of static excessive structure of a target system. The distribution of tasks among all components of cyberattacks on the system is often even, with a choice of components only according to their purpose. The increase of quantity and density of crisis situations' flow leads to structural complexity of systems designed to respond to them. This distributional design provides information redundancy of data and complication in its transfer and processing. The same principles are the basis for design of software aimed at realization of operational detecting processes, protection and active countermeasures to information threats in cyber space. The mentioned approaches are not efficient in real conditions of conflict where the enemy deploys equal or superior resources of information warfare, followed by soft power and kinetic forces to attain its objectives. This approach is a key feature of current hybrid wars.

Rigorous implementation of the principles of situational control provides opportunities for rational distribution and redistribution of own resources and focusing strengths on critical (for providing security) directions of enemy's actions. Methods of fractal analysis, self-organization and bifurcation models give an opportunity to detect threats and critical situations in time, predict the direction of their development and real objectives.

Practically, this approach increases the effectiveness of information warfare countermeasures as a result of advance warning systems, the completeness and accuracy of information, and timeliness of reactions.

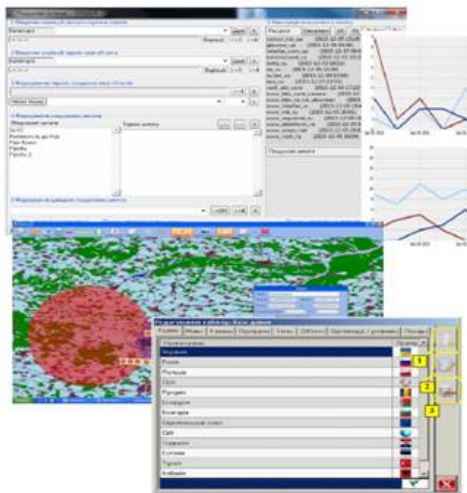


Photo 4. The formular view of one of the countermeasures complexes to psychological-information effects.

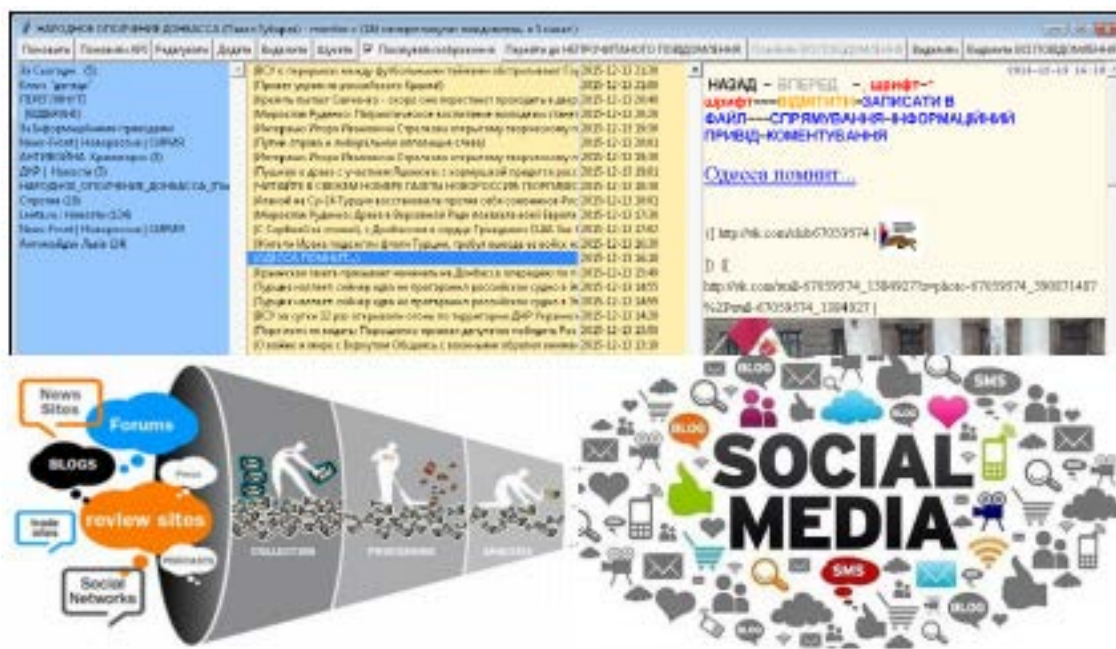


Photo.5 Automated system of information content-monitoring in social Internet services “Monitoring-C”.

Hybrid War Spheres

A crucial consideration is the impact of the actions of an aggressor desiring to increase internal instability in multiple spheres (Fig. 2). Intended impacts can include increasing distrust in institutions and shared values, erosion of economic activity and trust, and a confusion of objectivity, expertise, ideology, and other sources of social cohesion.^[34]

Hybrid wars differ significantly from traditional wars both in their initiation and prosecution, employing different strategies and means of operation. Hybrid warfare shares with irregular conflict (or IW – Irregular Warfare) the use of irregular or non-military forces, or at least those forces concealing their national allegiance in favor of anonymity or false camouflage as local militia. Special forces, sabotage-reconnaissance groups, intelligence units of various flavors are all involved in promoting and undertaking operations.^[35] For some armed forces or state security forces, special operations can involve conducting specific information or cyber-related activities, electronic operations, or sabotage actions designed to destroy critical nodes that cannot otherwise be achieved via traditional means.

A high priority for state defense under contemporary conditions is therefore the design of effective countermeasure systems. Such systems should include technologically advanced types of intelligence, electronic intelligence, information and psychological operations, and cyber operations that can be coordinated to achieve a common strategy, as well as being able to operate both independently and as part of other operations.

A key component of such independent operability in both ISR and combat operations is the development and use of unmanned drones. The increasing use of drones for different functional areas (intelligence, electronic countermeasures, direct strikes, etc.) and different operational environments (land, sea, air, amphibious) is an important consideration for flexibility in dynamic conflict situations.

Deployment of advanced intelligence and response capabilities must be developed in parallel with appropriate training for both military and civilian personnel who will need to work within the system. Technology cannot be expected to work properly without highly skilled personnel who can use, maintain, and further develop the complex systems needed to address the shifting nature of the battlefield. Full, effective

capabilities can only be expected when strategies and technologies are developed in coordination with professional training. The unprofessional use of such technologies is quite often the reason for their poor performance, as when standard operating procedures in training address much older conceptions of a problem (e.g. cyber intrusion into information networks as a technical issue, rather than a national security risk).

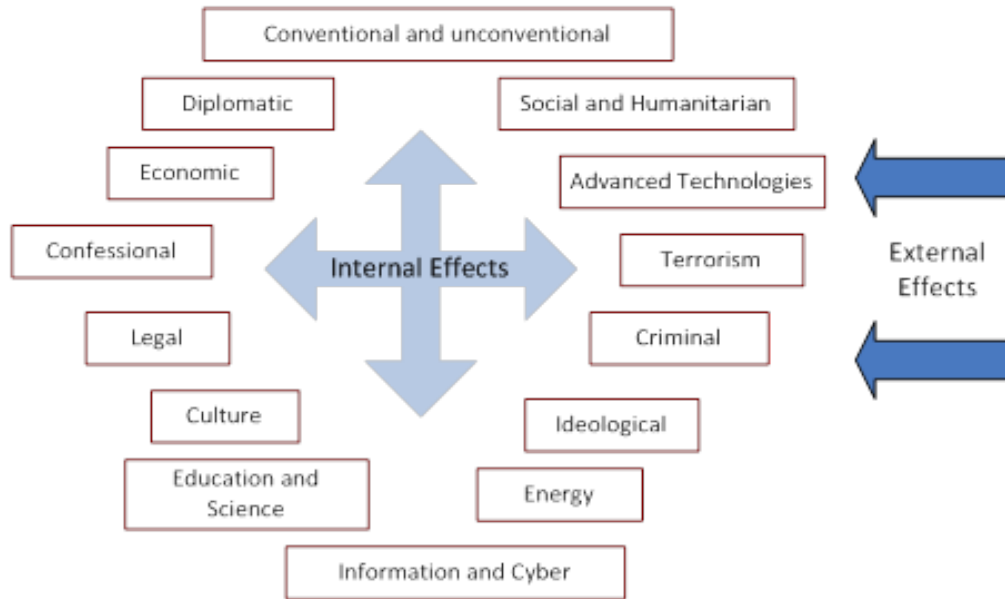


Figure 1: Hybrid War Spheres.

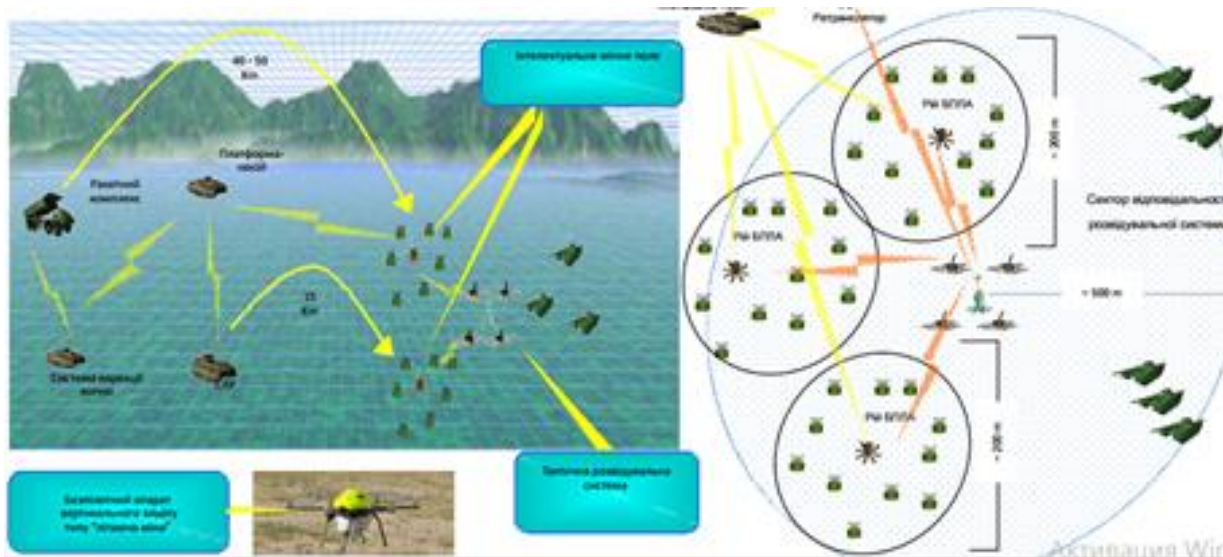


Photo 6. Unmanned Aircraft Complex of striking power for special operations like “Flying Mines.”^[36]



Photo 7. A screenshot from the electronic warfare planning system for planning the combat deployment of units.

The Advanced Defense Technologies Cluster

The state bears primary responsibility for the career management and training of defense personnel. Countries should therefore focus on the creation and development of technological defense systems, with integrated research and experimentation to provide appropriate levels of defense support. Extending the scope beyond the early warning available from ‘hybrid threat’ centers as established in some NATO countries, these clusters are intended to develop appropriate technologies and strategies for future threats they would be able to identify.

The envisioned Advanced Defense Technologies Cluster will include:

- A robust system of military research with proper scientific organizational structure
- Academic orientation toward expertise in advanced technologies
- Scientifically-based manufacturing complex, with stationary and mobile samples of weaponry and military equipment, command posts and laboratories
- Technologically advanced experimental combat and combat units, developed according to academic/scientific research of the cluster (Figure 2).

Practical military personnel training, testing and implementation of new technological systems of weaponry and military equipment, and the formation of new units must be based on developments by the defense technological cluster and active military units.

With respect to Ukraine, it is imperative to create a Military Scientific Technical Expert Center in advanced technological areas with the purpose of:

- avoiding double functioning of different organizations
- concentration in one place of efforts in research, design, creation, testing and use of advanced technological systems
- personnel training in areas of advanced technologies for all branches of the Armed Forces and for other ministries and establishments of the National Security and Defense Sector of the state
- use of the military component, industrial and manufacturing base of the region
- avoiding additional financial and temporary expenditures.

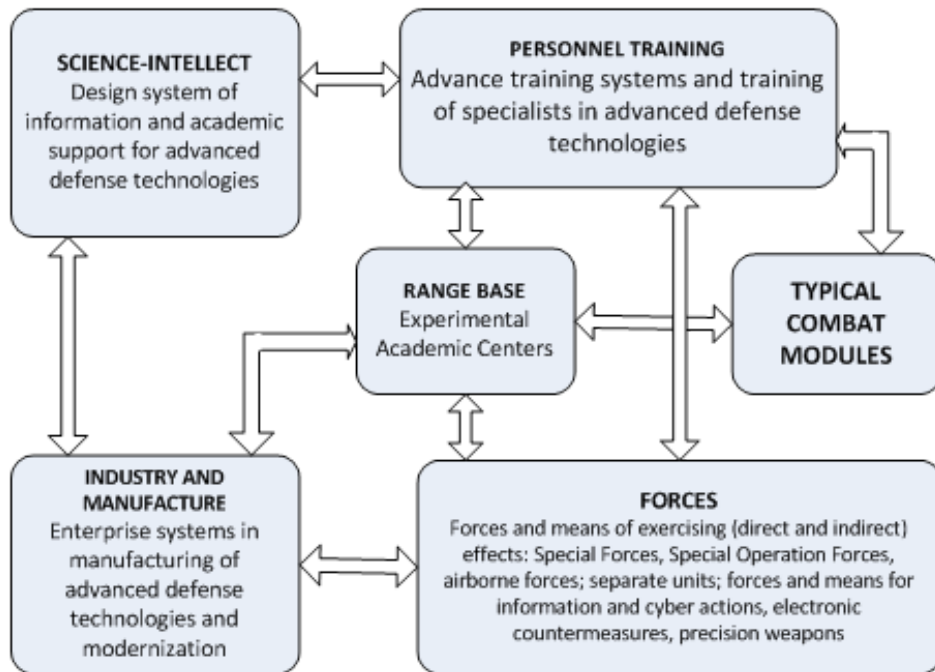


Figure 2: The Advanced Defense Technologies Cluster.

Practicability of the center can be substantiated and supported by relying upon experience of leading countries of the world gathered in the search of innovative ideas and their implementation in the military sphere, e.g. DARPA (the US Defense Advanced Research Projects Agency). Rational elaboration of all practical issues in the Advanced Defense Technologies Cluster must be conducted in close coordination with central military command and control organizations. It should work directly with forces cooperating with central control authorities. Central control authorities correspond with military units, and subdivisions with their range base and interacting organizations/ structures.

Conclusion

State policies of advanced technological, information and cyber security support systems have become among the most important components to consider with regards to national security policy in the military sphere. Modern technologies shift the ability to impact enemy forces, creating a need for reorganization to manage and defend against both soft and military effects, including in particular personnel training to maintain force readiness and continuity. The experiences of various countries that have already witnessed the new forms of hybrid warfare prove that national security and defense levels must be maintained even in conditions of world economic crisis and significantly decreased expenditures for the armed forces. The expansion of the battlefield beyond kinetic operations and infrastructure attacks demands complex use of both traditional force doctrines and new technological and synergistic planning.

The practice of military conflicts during the past decade demonstrates that the strategic advantage goes to the actor who first understands and implements new technologies, who can use them as a force multiplier and therefore overcome superior conventional forces – and often without even provoking a sustained response. Commanders must use the new methods, if only to understand the new methods and doctrines that the enemy can deploy. The use of advanced technological systems gives an opportunity to increase the effectiveness of already existing state military potential with lower expenditures, perhaps even by one third of traditional budgets. Considering the concepts of national security and national military strategies, governments of the most developed countries prioritize education and science for technologically intensive means of warfighting, implementing innovative control technologies, and providing for a fast and convincing victory in present and future military conflicts.

About the authors

Major General **Yuriy Danyk** is Professor and Doctor of Engineering Sciences. He graduated with honors from Zhytomyr Higher Military School of Radioelectronics, Kharkiv Military University (operational-tactical level), National Academy of Public Administration under the President of Ukraine, National University of Defense of Ukraine (operational-strategic level). He is an expert in the art of war, national defense and security, information and cyber security, electronic warfare, design and application of robotic complexes, and special forces development. He has combat experience in high technologies application.

E-mail: zhvinau@ukr.net([link sends e-mail](#))

Tamara Maliarchuk holds a M.Sc. degree. Since 2013 she works for S.Korolov Zhytomyr Military Institute and in 2014 became a PhD candidate in Ivan Franko Zhytomyr State University. In 2014-2016 she attended e-Learning forums and workshops (in National Defense Academies in Romania and Bulgaria) organized by NATO countries and Partnership for Peace in e-learning application. In 2015 Tamara graduated the Military English Phraseology Course of the National Defense Academy, Warsaw, Poland. In May 2016 she studied at the Defense Language Institute, Lackland, San Antonio, Texas, USA. She conducts research in e-learning, innovative technologies in PTSD detection and therapy, manipulative technologies in web-environment. *E-mail:* maliarchuktamara@gmail.com([link sends e-mail](#))

Dr. **Chad Briggs** is a Principal Consultant with Global INT. He has a PhD in political science from Carleton University in Canada, and specializes in translation of complex scientific data into risk assessments and strategic planning. He worked previously with the US Department of Energy on critical security assessments, and from 2010-2012 he was Minerva Chair of Energy and Environmental Security at the Air University, United States Air Force. He is a senior fellow at the Institute for Environmental Security in The Hague, professor of public policy at RIT Kosovo, and an adjunct professor of global security at Johns Hopkins University. *E-mail:* cbriggs9@jhu.edu([link sends e-mail](#)).

-
- [1] Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly* 52 (2009): 34-39.
 - [2] Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), <http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles>([link is external](#)).
 - [3] Volodymyr P. Gorbulin, Oleksandr S. Vlasiuk, Ella M. Libanova, Oleksandra M. Liashenko, *Donbas and The Crimea: The Value of Return* (Kyiv: National Institute of Strategic Studies, 2015); Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, <http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts>([link is external](#)) (31 August 2017).
 - [4] "Georgia 'overrun' by Russian troops as full-scale ground invasion begins," *Daily Mail*, <http://www.dailymail.co.uk/news/article-1043236/Georgia-overrun-Russian-troops-scale-ground-invasion-begins.html>([link is external](#)) (31 August 2017).
 - [5] See, for example, Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773-816, <https://doi.org/10.1080/01402390.2016.1273830>([link is external](#)).
 - [6] Patrick J. Buchanan, *The Death of the West: How Dying Populations and Immigrant Invasions Imperil Our Country and Civilization* (New York: St. Martin's Griffin, 2002).
 - [7] Andrew Monaghan, "The 'War' in Russia's 'Hybrid Warfare,'" *Parameters* 45, no. 4 (2015): 65-74.
 - [8] Brad Roberts, *Asymmetric Conflict 2010*, Report no. IDA-D-2538 (Alexandria, VA: Institute for Defense Analysis, 2000).

- [9] Vladimir Sazonov, Kristiina Müür and Holger Mölder, eds., *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Tartu: NATO Strategic Communications Centre of Excellence and Estonian National Defence College, 2016), <http://stratcomcoe.org/download/file/fid/7504>(link is external).
- [10] Elīna Lange-Ionatamišvili, *Redefining Euro-Atlantic Values: Russia's Manipulative Techniques* (Riga: NATO Strategic Communications Centre of Excellence, 2016), <http://stratcomcoe.org/download/file/fid/7350>;(link is external) Haroro J. Ingram, "Three traits of the Islamic State's information warfare," *The RUSI Journal* 159, no. 6 (2014): 4-11.
- [11] Ronald Inglehart and Pippa Norris, "Trump, Brexit, and the Rise of Populism: Economic Have-nots and Cultural Backlash," HKS Working Paper No. RWP16-026 (Harvard Kennedy School, 2016), <https://www.hks.harvard.edu/publications/trump-brexit-and-rise-of-populism-economic-have-nots-and-cultural-backlash>(link is external).
- [12] Samuel P. Huntington, "The Clash of Civilizations," *Foreign Affairs* 72, no. 3 (Summer 1993): 22-49.
- [13] The final argument of kings (a resort to arms).
- [14] Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013): 12-23 (in Russian).
- [15] See the Russian Military Technologies website, <http://www.rusarmy.com>(link is external), and the site of the "Russian Weaponry" Information Agency, <http://www.arms-expo.ru>(link is external).
- [16] Jānis Bērziņš, "Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy," *Policy Paper* no. 02 (Riga: Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014).
- [17] Yuriy G. Danyk, D. Ishchenko, O. Manko, "Military Aspects of Advanced Technological Systems' Classification," *S.Korolov Zhytomyr Military Institute Scientific Journal* 8 (2013): 5-13 (in Ukrainian).
- [18] Yuriy G. Danyk and O.O. Trush, "Specifics of Supporting National Security in an Environment of Advanced Technologies," *Government's Organization* 1 (2010), http://nbut.gov.ua/UJRN/DeBu_2010_1_42(link is external) (in Ukrainian).
- [19] Joseph S. Nye, "Soft Power," *Foreign Policy* 80 (Autumn 1990): 153-171.
- [20] David A. Deptula and James R. Marrs, "Global Distributed ISR Operations: The Changing Face of Warfare," *Joint Force Quarterly* 54 (2009): 110-115.
- [21] Brian Rappert, *Non-lethal Weapons as Legitimizing Forces? Technology, Politics, and the Management of Conflict* (Abingdon, UK: Routledge, 2003).
- [22] Frank G. Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis* 50, no. 3 (2006): 395-411.
- [23] Dan Madden, Dick Hoffmann, Michael Johnson, Fred Krawchuk, John E. Peters, Linda Robinson, and Abby Doll, *Special warfare: The Missing Middle in US Coercive Options*. (Santa Monica, CA: RAND, 2014).
- [24] Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (2015): 46-53.
- [25] Vasyl M. Telelim, D.P. Muzychenko, and Yu.V. Punda, "Force Planning for the 'Hybrid War' Scenarios," *Science and Defense* 20, no. 3 (2014): 30-35. (in Ukrainian).
- [26] For examples of the information operation to denigrate Ukraine's Armed Forces officials see "If only the Generals were not there," <http://www.segodnia.ru/content/168270>(link is external), <https://topwar.ru/85589-esli-by-ne-generalny-pozornaya-istoriya-ukrainskoy-armii.html>(link is external), <http://colonelcassad.livejournal.com/2474409.html>(link is external).
- [27] Duggan, "Strategic Development of Special Warfare in Cyberspace."
- [28] See, for example, <http://wartime.org.ua>(link is external).
- [29] InfoStream – News Monitoring Technology, <http://infostream.ua>(link is external).
- [30] Elizabeth Stoycheff and Erik C. Nisbet, "Priming the Costs of Conflict? Russian Public Opinion About the 2014 Crimean Conflict," *International Journal of Public Opinion Research* (2016): edw020. <https://doi.org/10.1093/ijpor/edw020>(link is external).
- [31] Duggan, "Strategic Development of Special Warfare in Cyberspace."
- [32] Sazonov, Müür and Mölder, eds., *Russian Information Campaign Against the Ukrainian State and Defence Forces*.
- [33] "Cyber Berkut," <https://cyber-berkut.org>(link is external), is an Internet brand, which covers hacker attacks mainly at governmental and civil web-resources of Ukraine. The head of the brand is unknown. The US specialist in Cyber Security, Jeffrey Car, considers it a group of Russian activists. The group describes its objectives, which include fight against neo-fascism, nationalism and the will of government in Ukraine. See also the TV Program on the First National TV channel of Ukraine "Black List of the Ukrainian Army" (part I), <https://www.youtube.com/watch?v=BAIDnaG4VeM>(link is external), and (part II), <https://www.youtube.com/watch?v=ksydsCllv0g>(link is external).

[34] Telelim, Muzychenko, and Punda, “Force Planning for the ‘Hybrid War’ Scenarios”; Kofman, “Russian Hybrid Warfare and Other Dark Arts”; Valeri Gerasimov, “The Value of Science in Prediction,” *Military Industrious Courier Journal* 8 (2013): 1-3 (in Russian).

[35] Gerasimov, “The Value of Science in Prediction.”

[36] This is a design of of the S.Korolov Zhytomyr Military Institute.

Parliamentary Attempts to Investigate Berlin's Vehicular Ramming Attack

Sebastian von Münchow; Lena Hantschke

Abstract:

On December 19th, 2016 Germany saw the first major Islamist terror attack on its soil. A Tunisian asylum seeker crashed a hijacked truck into one of the main Berlin's Christmas markets. The assault resulted in 12 casualties. In the aftermath, several attempts were made by German parliaments on Länder-level, as well as on federal level, to investigate how the terrorist was able to use 14 different identities, how he carried out the plot, how he escaped and where security authorities failed to prevent the attack.

Introduction

On the evening of December 19th, 2016, Anis Amri, a Tunisian asylum-seeker, hijacked a truck, killed the driver, and crashed into a Christmas market in Berlin. The Islamic State claimed responsibility for the attack, which resulted in twelve deaths and fifty additional casualties.^[1] Amri escaped the crime scene and travelled by train through Germany, the Netherlands, Belgium, and France to Northern Italy. In the morning of December 23rd, Italian police officers shot him dead in the town of Sesto San Giovanni, near Milan.

This assault was the first major Islamist terrorist event on German soil that resulted in the deaths of civilians.^[2] The attack re-heated the debate about Berlin's migration policy at large, but also focused on specific questions: How could Amri seek asylum in Germany despite his criminal record in Italy? How did he operate inside Germany using 14 different identities? How could Amri travel through five European countries before he was shot dead? ^[3] Throughout the state and federal levels, calls for security-related reforms,^[4] aimed at improving video surveillance, data exchange, increasing the staff of security agencies and tougher deportation procedures, flourished. In parallel, the question unfolded which legislative institutions could do a thorough *ex post* investigation of the plot? ^[5]

This contribution uses the Anis Amri case to illustrate the complexity of the German federative system, the diversity of law enforcement jurisdictions and respective parliamentary inquiries. It will not focus on the police aftermath reports, but instead will look at those investigations by ad hoc parliamentary committees which examine allegations of executive misconduct or failure. This brief discourse will help to understand the distinct jurisdictions of the states ("die Länder") and the federal level. Therefore, the paper elaborates on the parliamentary investigations from the City of Berlin as one of the 16 German states, then turns to the state of North-Rhine Westphalia (NRW) and subsequently introduces federal attempts where *ex post* investigations took place. Finally, the contribution will share some thoughts about the eventual achievements by the parliamentary endeavors to shed light on the attack.

Germany's Federative Security Structure

Maintaining public order and security in Germany falls under the jurisdiction of the 16 federal states. In consequence, Germany counts 16 departments of home affairs, 16 law enforcement agencies, 16 domestic intelligence services, 16 respective judicial bodies, and 16 different laws of public order. In the case of incidents that affect two or more states or have a transnational

dimension the Federal Criminal Police Office (Bundeskriminalamt – BKA), working under the auspices of the Ministry of Internal Affairs (Moi), can take charge if the legal requirements are satisfied.^[6] In 2004, the Joint Counter Terrorism Center (Gemeinsames Terrorismusabwehrzentrum, GTAZ) was founded as a fusion center where intelligence and law enforcement agencies of the federal and state level share their information. However, the GTAZ does not stand as a distinct authority itself. This is due to the “Trennungsgebot” which prevents intelligence authorities’ use of law enforcement instruments, such as placing someone under arrest.

State and Federal Inquiries

In terms of standing committees, an *ex post* investigation can be achieved via the internal affairs units on the federal and state levels. Additionally, the Parliamentary Control Panel (Parlamentarisches Kontrollgremium, PKGr) can conduct investigations on the federal level regarding topics related to the intelligence services. A special investigator can be appointed on the federal as well as on Länder-level.^[7] Such an investigator has the right to review files and talk to involved individuals.

Finally, a retroactive review of a case can also be conducted through the establishment of an ad hoc parliamentary committee of inquiry on the state or federal levels. This option provides the most powerful tools to reveal shortcomings and loopholes in the legal framework. The right to look into documents is far reaching, and questioning staff members from all hierarchical levels usually takes place in an open forum involving the press.^[8]

For the time being, several different inquiry committees have started their work on the Amri case on the state level. Nevertheless, an inquiry committee of the German Bundestag, dominated by the Grand Coalition between Conservatives and Social Democrats, has so far not been implemented.

Berlin

Like other crimes, terrorist attacks initially fall under the jurisdiction of the affected federal state. Berlin, like Hamburg and Bremen are cities, but enjoy each the status of a state in the federation of the total 16 states forming the Republic. Thus, Berlin’s Social Democratic Senator of Home Affairs and the State Police (the Landeskriminalamt, LKA) are the institutions in charge of investigating a plot executed in their city. Allegations against the LKA in regards to misjudging Amri as a danger caused the Berlin Landeskriminalamt and the Public Prosecutor’s Office Berlin to form the Taskforce “Lupe” (German for ‘magnifying glass’). The taskforce’s mandate was to examine whether the LKA case-workers and their supervisors played a role in the development leading to the fatal attack. Hence, this internal inquiry serves also to revisit control mechanisms within the structure of the LKA and may lead to additional disciplinary action against staff members.

Berlin’s Assembly and Internal Affairs Committee

The attack became the subject of debates in Berlin’s Assembly (Abgeordnetenhaus) and the Committee on internal affairs.^[9] The incident is still on the agenda and has so far been discussed in several meetings over the last few months, most recently on July 3rd, 2017.^[10] During this

session, a Special Investigator (see the next section) and a Head of the Counterterrorism Department of the Federal Public Prosecutor General presented their investigation's findings.

At the beginning of this hearing before Berlin's Committee on internal affairs, the Department Head of the Federal Public Prosecutor stressed that his appearance before the Committee had an exceptional character. He argued that he is only obliged to appear before a competent forum of the German Bundestag. Indeed, his cooperation is based on good will. The Department Head represents a federal authority and cannot be forced by the committee on Länder-level to appear as a witness. In consequence, the Berlin members of the committee could not directly address him with questions during the meeting. The questions had to be submitted in advance. The Department Head of the Federal Public Prosecutor summarized the current state of the ongoing investigation and thereafter only answered selected questions. He also mentioned several transnational elements of the attack. First, Anis Amri was in continuous contact with at least one foreign IS-member via text messages while conducting the attack. Second, there are hints of further possible confidants or accomplices in other nations. Third, the weapon he used can be traced back to Switzerland. In this light there have already been investigations in other states. Eurojust, a European network of public prosecutors, was involved. Mutual legal assistance requests were sent to Belgium, the Netherlands, Great Britain, Italy, Austria, Poland, Switzerland, Spain, France, Tunisia and the U.S.A.

Special Investigator

Berlin's Social Democrat, Socialist and Green Party-led city government, the "Senat," appointed Mr. Bruno Jost as a Special Investigator. As a retired prosecutor, he was thought to be the best to handle this task and submit findings to the committee. He started work in April 2017. A final report is expected in October 2017.^[11] Mr. Jost presented an interim report to the aforementioned committee session on July 3rd, 2017.

During the investigation, the focus shifted from examining the general preconditions that allowed the attack to happen to the review of report by the LKA Berlin, which might have been subsequently edited. It was alleged that the editing took place to cover mistakes by the LKA that prevented the detention of Amri before the attack happened. This particular aspect is indirectly linked to the question of possible surveillance of Amri by the security authorities. However, the report was alleged to have been edited in January 2017 after the vehicular ramming attack. Hence, the LKA Berlin was accused of rewriting the findings to its favor. The interim report stated there was a police note about Amri acting as a drug dealer from November 1st, 2016. This first version concluded that Amri and collaborators were dealing drugs on a large scale. The important observation would have been sufficient to justify further surveillance, or even the issuance of an arrest warrant. According to the procedures, this observation should have been sent to the Public Prosecutor's Office in Berlin for further decisions on actions against Anis Amri. Nevertheless, this did not happen. Instead the second version appeared in January 2017. The findings by the Special Investigator suggest that this paper dated back to November 1st, 2016 and has elements different from the first edition. It stated that Amri only dealt drugs on a very low level, and did not mention any accomplices. This portrayal could not have been a justification for further surveillance or even an arrest warrant. Thus, the LKA Berlin was confronted with the accusation that it unintentionally prevented further actions against Amri by not forwarding the first report to

Berlin's Public Prosecutor's office. This led to the above-mentioned criminal investigations against the involved police officers due to the suspicion of document fraud.[\[12\]](#) To this day, this aspect is subject to speculation since the allegation is built upon the assumption that the Public Prosecutor's Office would have led to further surveillance or an arrest of Amri.

In his hearing at the Standing committee of home affairs at the Berliner Abgeordnetenhaus on July 19th 2017, the Special Investigator said that he is currently focusing on this aspect. He also promised to take a deeper look into other related questions of eventual misconduct before submitting the final report.[\[13\]](#)

Another interesting part of the findings of the Special Investigator in Berlin is that they differ slightly from the findings of the Special Investigator in North Rhine-Westphalia. In particular, Mr. Jost stated that Amri could have been arrested to secure his return to Tunisia. The Asylum Act states an arrest is lawful in cases where the removal of the foreigner seems possible in due time,[\[14\]](#) which is only the case when citizenship is being confirmed. For individuals who enter Germany without a passport, the so-called PEP-procedure (Passersatzpapiere, PEP) intends to verify their nationality and identity. This procedure enables authorities to approach the assumed country of origin to confirm the identity and citizenship. Tunisian authorities responded in October 2016 [\[15\]](#) confirming Amri's identity, origin, and citizenship. Consequently, a detention would have been lawful. The NRW Special Investigator concluded that the detention of Amri would not have been in accordance with the Act at any stage of the events (see next section).

Ad hoc Inquiry Committee

Berlin's Assembly also formed an ad hoc inquiry committee on the incident. It started its work on July 14th, 2017.[\[16\]](#) Due to the parliamentary summer break there are no work results yet.

North Rhine-Westphalia

Amri registered as an asylum seeker in NRW and was partly surveilled by state security authorities. Unlike Berlin, the NRW deputies established two parliamentary inquiries. A brief, but intense ad hoc investigation took place under the former Social Democrat-Green Coalition from February until May 2017; a second was launched on July 1st, 2017 [\[17\]](#) after a Conservative-Liberal government took office in the beginning of June 2017. Given that the inquiry mandates in two *Länder* take place under two separate jurisdictions, the parliamentarians need to rely on a voluntary exchange of files between the respective entities in Berlin and NRW's capital Düsseldorf, as well as on the good will of any federal institution.

House of Deputies

As in Berlin's Assembly, the attack was also subject to debates in NRW's House of Deputies, the Landtag, and the respective committee on internal affairs.[\[18\]](#) The issue was discussed in several ad hoc meetings of the committee. Several representatives of security bodies were invited to answer questions related to the case and Amri's record in NRW.[\[19\]](#)

Special Investigator

A Special Investigator was also in charge of examining Amri's deadly course of action. NRW's state government assigned a criminal law professor to serve in this position.[\[20\]](#) The scholar's report found that the authorities in NRW did not make crucial mistakes. On the contrary, he continues,

NRW state police warned Berlin authorities about a potential risk of a terrorist attack conducted by Amri. According to this view, the authorities in Berlin ignored the warning.

The professor did not clearly point out under which circumstances NRW warned Berlin about Amri. It was discovered that Amri was discussed in several meetings of the Berlin-located GTAZ. NRW security staff participated in those meetings [21] and stressed Amri's potential on February 17th, 2016. Contrary to this opinion, the representatives of the federal police, the BKA, assessed the danger as unlikely.[22]

As mentioned before, the Special Investigator also said that Anis Amri could not have been taken into custody after his asylum application was rejected.

Ad hoc Inquiry Committee

In light of the public outrage about the case, a demand to establish an ad hoc inquiry arose.[23] The committee was established by NRW's House of Deputies on February 15th, 2017.[24] In spring 2017, this inquiry developed as the first key arena to shed light on the plot. It quickly assessed the available documents and summoned home ministers, including the Federal Minister for Home Affairs Thomas de Maizière (Conservative Party). Ad hoc inquiry committees are subject to the principle of discontinuity. This means that they last as long as the legislative term.[25] Accordingly, the NRW committee came to an end due to elections in NRW in May 2017. The NRW committee published a 175-page interim report in April 2017. Nevertheless, this report does not contain a final statement on the findings but only provides the current state of the inquiry. The newly elected NRW parliament set up a new inquiry committee which started work in June [26] and has so far only held an initial meeting.

Federal Level

The question remains if a federal inquiry committee would have been able to provide the full picture of the incident.[27] The Breitscheidplatz attack proved that some security-related questions go beyond nation- and interstate borders. Moreover, the roles of the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge, BAMF) as Germany's central authority dealing with refugees as well as the federal authorities gathered in the GTAZ, such as the Federal Criminal Police Office (BKA), the Federal Intelligence Service (Bundesnachrichtendienst, BND) and the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) seem to deserve an examination. A pure Länder-focused approach could miss transnational components of the plot like Amri's criminal past in Italy and the track he chose escaping to Milan. Since the 16 states have a limited ability to deal with foreign affairs, the international entanglement suggests the involvement of Germany's federal level.[28]

Federal decision-makers quickly realized that some sort of *ex post* investigative attempts by the German Bundestag were due. In January 2017, the Parliamentary Control Panel (Parlamentarisches Kontrollgremium, PKGr) began to discuss the incident in the light of possible errors by the intelligence service.[29] An ad hoc parliamentary inquiry committee of the German Bundestag has so far not been set up.

Internal Affairs Committee

The Bundestag's committee on internal affairs discussed the issue in several non-public meetings, *inter alia* on January 18th and February 13th, 2017. During the meeting in February, the Ministers of Home Affairs of Berlin and NRW as well as the heads of the BND, the BfV, the BKA and other authorities were questioned. The committee and the authority's representatives discussed different legislative proposals, such as the modification of the Asylum Act.^[30] A Member of the Internal Affairs Committee pointed out that the state level cannot solely be blamed for failures in the Amri case. He also stressed a responsibility of the federal level and kept lobbying for the establishment of a parliamentary inquiry.^[31]

Parliamentary Control Panel

In a special meeting on January 16th, 2017 the PKGr sub-assigned the former Head of Germany's Mol Legal and General Affairs of Public Security Department, Arne Schlatmann, to investigate the plot. His work was accompanied by four PKGr members from different parties.^[32] The findings were submitted to the German Parliament in an open final report on May 31st, 2017.^[33] Since the PKGr has no supervisory power over aspects that fall under the jurisdiction of the states, the report covers only action or inaction of federal entities like the BKA, the BfV, and the BND. According to the PKGr, those agencies had only had a supporting function in the Amri case. The main security actors were the competent authorities in the state of NRW and the City of Berlin, as well as the competent institutions gathered in the GTAZ. The PKGr concludes that those authorities should have recognized Amri's potential. Therefore, the PKGr wondered why no further actions against Amri were taken to prevent the attack. The Panel also criticized Amri's mobility within Germany causing different judgments by different authorities. The report highlighted the shortcomings of the immigration authorities in not taking further action to detain Amri after his application for asylum was rejected.

Ad hoc Committee of Inquiry

As stated above, an ad hoc parliamentary inquiry committee of the German Bundestag was not set up. The refusal to review the case on the federal level is surprising in light of the intense public debates usually sparked by inquiries, the past record of conducted inquiries and the far-reaching legal rights of the members of Parliament to assess files and to question officials including ministers and the Chancellor. The Bundestag would have had the time in January 2017 to launch an investigation since the federal elections were scheduled for September 2017. The deputies in Düsseldorf made the attempt and could at least review files and summon some major witnesses in a much shorter time between February and April 2017.

To understand the full potential of an ad hoc committee of inquiry as an adequate tool to review incidents like the Berlin attack, a short look into the legal framework and the political background of such investigations is helpful. Ad hoc committees are meant to find governmental misconduct or legal violations by gathering and evaluating evidence and to provide recommendations to prevent further fault. The implementation of ad hoc inquiry committee by a qualified minority of the parliament is the most intense constitutional tool of Germany's legislative bodies because they foster public debate about the case, the performance of the involved security agencies, and the entire applicable legislative set-up related to the plot. The

selected members of a parliamentary committee of inquiry enjoy unrestricted access to classified material and benefit from the witnesses' duty to appear at the hearings.[\[34\]](#)

When looking at the ad hoc committees of inquiry since Germany's reunification, the ratio of security versus non-security topics investigated yields a higher ratio than expected. Six particular investigations into such areas as energy safety, political party financing, wide-spread diseases, and bad bank scandals took place since Germany's reunification in 1990. In the same period, twelve inquiries focused on alleged misconduct by security bodies. Amongst the best known inquiries were the investigations on the role of BND staff in Bagdad during the 2003 Iraq War, alleged German involvement in rendition cases, an air strike against hijacked fuel tanks near a German Army camp in Kunduz, Afghanistan, the failure of security authorities to stop serial murders by a Neo-Nazi trio,[\[35\]](#) as well as the impact of the so-called Snowden Leaks and Berlin's eventual collaboration.[\[36\]](#) In sum, security matters are investigated twice as often as non-security issues. This ratio suggests that the security agencies themselves constitute the biggest threat to Germany and its citizens. Following this legacy, the Amri case would have perfectly suited the Bundestag's appetite to investigate security sector misconduct. For some reason this did not take place, leaving a bitter taste and suspicion that the very constellation of the Breitscheidplatz plot was perceived as politically inconvenient to establish a thorough *ex post* investigation.

Achievements

Returning to the plot, the record of the fora of inquiry on the state level is mixed. Certainly, the blame game between the security architectures in the City of Berlin, Düsseldorf, and from the federal level have not contributed to public trust in the functioning of German law enforcement or intelligence authorities. Consequently, Federal Minister for Home Affairs Thomas de Maizière said: "in cases like Amri we urgently need more commitment and unity among the authorities of the federal government and the states." This statement was widely criticized by the respective Ministers on the Länder-level.[\[37\]](#) They feared that the genuine power to maintain public order and security on the Länder-level was intended to be undermined to the advantage of the federal level. Hence, the challenge is to strike a balance between promoting cooperation and aligning police work while maintaining the federalist separation of power.

An example may illustrate the background of this state-federal level mistrust. The term "Gefährder" describes a person who is believed to have the potential to conduct a terrorist attack. The term exists in all respective state legislation. What differs is how state officials interpret the term "Gefährder." While the threshold could be low in some states, it may be high in others. A standard understanding does not exist. Consequently, the federal level started to call for a common approach to defining terms like "Gefährder." This very call made ministers on the state level fear an emerging federal power patronizing Länder-police work. This overlooks that the federalist system could in fact be strengthened. A common understanding between state and federal authorities does not mean that law enforcement agencies on the Länder-level lose their capabilities to operate in their territorial jurisdictions. The different levels are best reconciled when understanding the mutual benefit from enhanced communication, cooperation and applying common definitions.[\[38\]](#)

The case also kicked in some reforms to prevent similar attacks in the future. First, a law to improve the data exchange between the authorities of the states (Datenaustauschverbesserungsgesetz) came into force. This should help preventing possible attackers from using different identities to apply for asylum in different states in Germany.[39] Second, a system for a standardized risk analysis of certain persons was implemented. The work on the RADAR-iTE system [40] was already finished in September 2016 and has been gradually implemented by summer 2017. The aim is to provide a standardized risk analysis tool for the relevant entities on state and federal level. Third, the vehicular ramming attack boosted a bilateral understanding to return Tunisian nationals who have not been granted asylum in Germany. This system is currently being utilized on a bilateral level between Tunisia and Germany.[41]

Finally, a new legal framework empowers the BKA with more efficient tools to fight terrorists. The use of ankle restraints was introduced. The procedure to arrest potential attackers who are obliged to leave the country was eased. All these developments had already begun before the vehicle ramming attack. But the Breitscheidplatz plot caused the political dynamics to strengthen Germany's security structure. Other reforms are still on the agenda, e.g. improving data exchange between the 16 German states as well as between the Federal Republic and third countries or countering radicalization of individuals in Germany.[42]

Conclusion

Beyond Germany's 2017 pre-national election's atmosphere, it remains speculative to find reasons why an inquiry on federal level was refused. Ad hoc inquiries have exposed wrongdoings and uncovered severe deficiencies in the past 27 years, although the final reports have rarely suggested that German officials violated national or international law. Usually these inquiries lead to stronger parliamentary control over the security sector. In addition, many intra-agency restrictions were introduced. These restrictions received criticism for having immobilized the security sector's capabilities to a critical degree in the past decades. In parallel, a large scale-down of military, police and intelligence staff put further pressure on the capacity of the security sector. Hence, a parliamentary investigation of the Amri case could have revealed the following: Legislative and staff constraints immobilized the German security architecture in a way that it was unable to tackle a radicalized Tunisian.

In sum, the work of the Special Investigators and the parliamentary inquiries have exposed many disadvantages of Germany's security architecture. While some needed reforms were introduced, Germany did not develop a blind ambition to introduce instruments that unnecessarily restrict civil rights and liberties. Most importantly, the attack did cause a public debate about readjusting counter-terrorism shortcomings with a focus on cooperation between different Länder and federal authorities. This might empower the affected agencies to function in the light of a statement made by Thomas de Maizière right after the Breitscheidplatz attack: "The state is not the adversary of a free society but its instrument [...]. The democratic state doesn't threaten freedom, it protects it." [43]

The views expressed in this paper are solely those of the authors and do not reflect those of any institution.

About the authors

Dr. **Sebastian von Münchow** is a lecturer at the George C. Marshall European Center for Security Studies. He studied law and political science in Berlin, Lausanne and Vienna. After receiving the Masters of Law, he became a member of the Berlin bar. He earned his doctorate in international relations from the University of Vienna. Dr. von Münchow then worked for the field missions of the Organization for Security and Co-operation in Europe in Bosnia and Herzegovina, as well as in Kosovo. He has also served in the Police Assistance Mission of the European Community in Tirana. In Brussels, he joined the Office of the Special Coordinator of the Stability Pact for South Eastern Europe. After returning to Berlin, Dr. von Münchow worked for the German Government.

E-mail: sebastianvonm@marshallcenter.org(link sends e-mail).

Lena Hantschke studied law at Humboldt University Berlin. She received the Masters of Law in 2015 and worked for the research service of the German Parliament, Bundestag. Ms. Hantschke then became a legal clerk at the Berlin Supreme Court, which seconded her to the Marshall Center in summer 2017. Lena Hantschke recently became a member of the Berlin bar. Her Ph.D. will focus on current challenges to the German security architecture.

E-mail: LL.Hantschke@hotmail.com(link sends e-mail).

[1] “OSINT Summary: Vehicle impact attack on Berlin Christmas market highlights increasing adoption of tactic,” *IHS Jane's Terrorism & Insurgency Monitor*, December 20, 2016, <http://janes.ihs.com/TerrorismInsurgencyCentre/Display/1791686>(link is external).

[2] There was one attack in March 2011 in Frankfurt. It is considered to have an Islamist background. Arid Uka, a presumed self-radicalized youngster of Kosovar origin, killed two U.S. airmen and wounded two others when they wanted to board a plane at Frankfurt Airport. For further information on the incident see “Frankfurt Airport shooting: two US-serviceman dead,” *BBC News online*, March 2, 2011, www.bbc.com/news/world-europe-12621832(link is external), and “Frankfurt airport gunman jailed for life,” *BBC News online*, February 10, 2012, www.bbc.com/news/world-europe-16984066(link is external).

[3] “Berlin truck attack: Can the EU stop another Amri?” *BBC News*, January 6, 2017, <http://www.bbc.com/news/world-europe-38517768>(link is external). See also “The Berlin Vehicular Ramming Attack – What we know & Insights from ICT Experts,” *The*

International Institute for Counter-Terrorism (ICT) online, December 22, 2016, www.ict.org.il/Article/1883/the-berlin-vehicular-ramming-attack(link is external).

- [4] “Gegen Terrorismus hilft nur Besonnenheit,” *Der Tagesspiegel online*, February 2, 2017, www.tagesspiegel.de/politik/gesetzentwurf-zu-fussfesseln-gegen-terrorismus-hilft-nur-besonnenheit/19335506.html(link is external). Note the intention to introduce an early warning mechanism called RADAR: “Neues System zur besseren Gefährder-Einschätzung,” *Berliner Zeitung online*, January 21, 2017, <http://www.berliner-zeitung.de/politik/neues-system-zur-besseren-gefaehrder-einschaetzung-25588238>(link is external). NRW law enforcement reform plans: “Was die Polizei in NRW verbessern will,” *Spiegel online*, February 13, 2017, <http://www.spiegel.de/politik/deutschland/anis-amri-was-die-polizei-in-nrw-nach-anschlag-in-berlin-verbessern-will-a-1134309.html>(link is external).
- [5] “Sicherheitsdebatte: Souverän gegen Terror,” *FAZ online*, January 11, 2017, www.faz.net/aktuell/politik/inland/sicherheitsdebatte-souveraen-gegen-terror-14613401.html(link is external). See also Federal Minister for Internal Affairs, Thomas de Maizière’s statement “Sicherheit als gemeinsame Verantwortung,” *Bundesregierung*, January 28, 2017, <https://www.bundesregierung.de/Content/DE/Interview/2017/01/2017-01-28-de-maiziere-spiegel.html>(link is external).
- [6] The legal requirements are defined in the statute of the German Federal Police (Bundeskriminalamtgesetz, BKAG, § 4).
- [7] The legal basis for the appointment of a special investigator is article 10 of the Law of the Committees of Inquiry (Paragraph 10 Parlamentarisches Untersuchungsausschussgesetz, PUAG) on federal level. It corresponds with similar legislation on state level. The government (be it state or federal level) can appoint a special investigator via its governmental authority. The appointment of a special investigator by the executive branch cannot prevent the legislative branch from fully exercising its investigative rights, e.g. implementing an *ad hoc* inquiry committee.
- [8] The chairman of the Christian Democratic Union fraction Mr. Volker Kauder declared to be in favor of an ad hoc inquiry committee by the German Bundestag. He would suggest this to his Social Democrat counterpart, Mr. Thomas Oppermann. See Martin Lutz and Constanze Reuscher, “Anis Amri soll regelmäßig Drogen genommen haben,” *Welt online*, January 15, 2017, www.welt.de/politik/deutschland/article161179412/Anis-Amri-nahm-regelmaessig-Ecstasy-und-Kokain.html(link is external).
- [9] “Berliner Anschlag: Verhalte Warnungen aus Marokko,” *Telepolis*, January 31, 2017, www.heise.de/tp/news/Berliner-Anschlag-Verhalte-Warnungen-aus-Marokko-3611242.html(link is external). See also “Terroranschlag erneut einziges Thema im Innenausschuss,” *Berliner Morgenpost online*, January 22, 2017, www.morgenpost.de/berlin/article209356113/Terroranschlag-erneut-einziges-Thema-im-Innenausschuss.html(link is external).
- [10] See protocol of the meeting, July 3, 2017, www.parlament-berlin.de/C1257B550(link is external) 02AD428/CurrentBaseLink/W29ASL7D644DEVSD?Open&Wahlperiode=18&Vorgang=0023&Ausschuss=Ausschuss für Inneres, Sicherheit und Ordnung.

- [11] “Ex-Bundesanwalt Jost wird Sonderermittler im Fall Amri,” *BerlinOnline*, April 3, 2017, <https://www.berlinonline.de/aktuell/4811000-4015970-exbundesanwalt-jost-wird-sonderermittler.html>; (link is external) and “Amri-Sonderermittler klagt über Probleme bei der Akteneinsicht,” *Der Tagesspiegel online*, May 16, 2017, www.tagesspiegel.de/berlin/polizei-justiz/attentat-am-breitscheidplatz-in-berlin-amri-sonderermittler-klagt-ueber-probleme-bei-d... (link is external).
- [12] “Anschlag in Berlin – weitere Manipulationen an Akte Amri,” *Zeit online*, May 21, 2017, <http://www.zeit.de/politik/deutschland/2017-05/anschlag-berlin-anis-amri> (link is external) lka-manipulation-akten.
- [13] See protocol of the meeting of the committee of home affairs Berliner Abgeordnetenhaus, July 19, 2017, <https://www.parlament-berlin.de/C1257B55002AD428/> (link is external) CurrentBaseLink/W29ASL7D644DEVSDE?Open&Wahlperiode=18&Vorgang=0085&Ausschuss=Ausschuss für Inneres, Sicherheit und Ordnung.
- [14] The legal requirements are defined in the German Asylum Act (Aufenthaltsgesetz, AufenthG, § 62 Abs. 3 S. 3).
- [15] Germany’s federal Minister for Home Affairs Thomas de Maizière said that Tunisian authorities confirmed Amri’s identity in October 2016: “De Maizière zum Fall Amri - Antrag auf Abschiebehaft hätte gute Erfolgsaussichten gehabt,” *SpiegelOnline*, January 28, 2017, www.spiegel.de/politik/deutschland/thomas-de-maiziere-anis-amri-haette-in-abschiebehaft-genommen-werden-koennen-a-1132010.html (link is external). Berlin’s Special Investigator stated that Amri’s identity was confirmed already in August 2016; see protocol of Berlin’s assembly meeting on July 3, 2017, www.parlament-berlin.de/C1257B55002AD428/CurrentBaseLink/W29ASL7D644DEVSDE?Open&Wahlperiode=18&Vorgang=0023&Ausschuss=Ausschuss (link is external) für Inneres, Sicherheit und Ordnung.
- [16] See press release of the Berlin Assembly, July 11, 2017, <https://www.parlament-berlin.de/C1257B55002AD428/vwContentByKey/W2AP6F5Y454WEBSDE> (link is external).
- [17] See press release of NRW’s house of deputies, July 1, 2017, www.landtag.nrw.de/portal/WWW/GB_II/II.1/Pressemitteilungen-Informationen-Aufmacher/Pressemitteilungen-Informationen/Pressemitteilungen/2017/06_neues_Impressum/Untersuchungsausschuss_%26%23132Fall_Amri%26%23147_eingesetzt.jsp.
- [18] “NRW-Ausschuss diskutiert Berliner Attentat: Anis Amri nutzte 14 Identitäten,” *Der Spiegel online*, January 5, 2017, www.spiegel.de/politik/deutschland/anschlag-in-berlin-ralf-jaeger-aeussert-sich-zu-anis-amri-a-1128697.html (link is external). See also “Nach Anschlag in Berlin: Die Gefährlichkeit des Anis Amri,” *FAZ online*, January 5, 2017, <http://www.faz.net/aktuell/politik/rechtfertigung-von-innenminister-jaeger-wegen-anschlag-14606371.html>; (link is external) and “Tunis will Kontaktmann Amris anklagen,” *Der Spiegel online*, January 2, 2017, <http://www.spiegel.de/politik/ausland/anis-amri-tunesien-will-kontaktmann-anklagen-a-1132958.html> (link is external).
- [19] See protocols of the special meetings No. 101, January 5, 2017; 103, January 19, 2017; 105, February 2, 2017, <https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD16-1564.pdf>; (link is

external) www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD16-1582.pdf;(link is external) www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD16-1594.pdf(link is external).

- [20] “Kraft setzt Sonderermittler im Fall Amri ein,” *Zeit online*, January 25, 2017, <http://www.zeit.de/politik/deutschland/2017-01/nordrhein-westfalen-hannelore-kraft-anis-amri-berlin-attantaeter-sonderermittlung>(link is external). See also “Sonderermittler soll Fall Amri aufklären,” *Handelsblatt online*, January 25, 2017, www.handelsblatt.com/politik/deutschland/nach-berlin-anschlag-sonderermittler-soll-fall-amri-aufklaeren/19301674.html(link is external). Hinting at the establishment of an ad hoc parliamentary inquiry: “Politik Kompakt I,” *Welt online*, February 8, 2017, www.welt.de/print/die_welt/politik/article161895769/Politik-Kompakt-I.html;(link is external) and “Ausschuss in NRW soll Fall Amri untersuchen,” *Zeit online*, February 7, 2017, <http://www.zeit.de/politik/deutschland/2017-02/anschlag-breitscheidplatz-anis-amri-landtag-duesseldorf-untersuchungsausschuss>(link is external). Kretschmer submits controversial report: “Fall Amri: Grüne attackieren Krafts Gutachter,” *Express online*, March 30, 2017, www.express.de/news/politik-und-wirtschaft/fall-amri-gruene-attackieren-krafts-gutachter-26284776(link is external).
- [21] “Terrorfall Amri – Sonderermittler entlastet die Behörden in NRW,” *Der Tagesspiegel online*, March 27, 2017, <http://www.tagesspiegel.de/politik/terrorfall-amri-sonderermittler-entlastet-die-behoerden-in-nrw/19577652.html>(link is external).
- [22] “Berlin Attack: An Attack is Expected,” *Zeit online*, April 5, 2017, www.zeit.de/politik/deutschland/2017-04/berlin-attack-christmas-market-breitscheidplatz-anis-amri(link is external).
- [23] “Verfassungsschutz belastet Landeskriminalamt,” *rbb24*, February 9, 2017, www.rbb-online.de/politik/beitrag/2017/02/Verfassungsschutz-Palenda-schiebt-Schuld-im-Fall-Amri-von-sich.html(link is external).
- [24] “NRW beschließt Untersuchungsausschuss zum Fall Amri,” *Der Tagesspiegel online*, February 15, 2017, www.tagesspiegel.de/politik/berlin-attantaeter-nrw-beschliesst-untersuchungsausschuss-zum-fall-amri/19396466.html(link is external).
- [25] On the function and rights of the Parliamentary Control of the Intelligence Services see Dietmar Peitsch, Christina Polzin, “Die parlamentarische Kontrolle der Nachrichtendienste,” *Neue Zeitschrift für Verwaltungsrecht* 4 (2000): 387–93. Inquiries usually end by submitting a report with recommendations to the Speaker of Parliament.
- [26] “Terrorfall Amri: Ausschuss im neuen NRW-Landtag nahm Arbeit auf,” *Westdeutsche Zeitung online*, June 27, 2017, <http://www.wz.de/home/politik/inland/landtagswahl-nrw/terrorfall-amri-ausschuss-im-neuen-nrw-landtag-nahm-arbeit-auf-1.2463395>(link is external).
- [27] “Rufe nach Neuorganisation der Terrorabwehr,” *Handelsblatt online*, February 2, 2017, <http://www.handelsblatt.com/politik/deutschland/berliner-terroranschlag-rufe-nach-neuorganisation-der-terrorabwehr/19269704.html>. See also “Fall Amri: Neue Antworten – neue Fragen,” *Berliner Morgenpost online*, February 3, 2017, <http://www.morgenpost.de/politik/article209485027/Fall-Amri-Neue-Antworten-neue-Fragen.html>. Berlin/Düsseldorf blame game: “NRW-Landesregierung muss sich

- kritische Fragen gefallen lassen,” *FAZ online*, February 13, 2017, <http://www.faz.net/aktuell/politik/kritik-an-nrw-innenminister-jaeger-fall-anis-amri-14876497.html>(link is external).
- [28] “Der Antiterrorkrampf,” *Der Spiegel online*, January 22, 2017, www.spiegel.de/spiegel/anis-amri-und-der-anschlag-von-berlin-ermittlungspannen-keine-aufklaerung-a-1131008.html. See also “Polizei führte Anis Amri kurz vor der Tat als Terrorist,” *Der Tagesspiegel online*, January 16, 2017, www.tagesspiegel.de/politik/attentat-auf-breitscheidplatz-polizei-fuehrte-anis-amri-kurz-vor-der-tat-als-terrorist/19259836.html; and “Italiens Behörden verschwiegen schwere Panne im Fall Amri,” *Welt online*, January 22, 2017, www.welt.de/politik/deutschland/article161386891/Italiens-Behoerden-verschwiegen-schwere-Panne-im-Fall-Amri.html(link is external).
- [29] On the function and rights of the Parliamentary Control of the Intelligence Services see: Dietmar Peitsch, Christina Polzin, “Die parlamentarische Kontrolle der Nachrichtendienste,” *Neue Zeitschrift für Verwaltungsrecht* 4 (2000): 387–93.
- [30] See press release of the German Bundestag, February 13, 2017, www.bundestag.de/presse/pressemitteilungen/2017/pm-170209-pm-amri/492512(link is external).
- [31] *Ibid.*
- [32] The legal base for this procedure is § 1 Absatz 1 in conjunction with § 5a PKGr – statute (Kontrollgremiumgesetz).
- [33] “Unterrichtung durch das Parlamentarische Kontrollgremium,” *Bundestag Drs.* 18/12585, May 31, 2017, <http://dip21.bundestag.de/dip21/btd/18/125/1812585.pdf>(link is external).
- [34] Sebastian von Münchow, “Security Agencies and Parliamentary Committees of Inquiry in Germany: Transparency vs. Confidentiality,” *Connections: The Quarterly Journal* 12, no. 4 (2013): 51–74, <https://doi.org/10.11610/Connections.12.4.03>(link is external).
- [35] The NSU (“National Socialist Underground”) was a right-wing terrorist group which managed to remain undetected for more than a decade. The final report of the Committee is available at <http://dip21.bundestag.de/dip21/btd/18/129/1812950.pdf>(link is external).
- [36] The final report of the Committee is available at <http://dip21.bundestag.de/dip21/btd/18/128/1812850.pdf>(link is external).
- [37] “Um die Vorschläge von Innenminister de Maizière ist ein heftiger Streit entbrannt – das sind die Fakten,” *The Huffington Post*, April 1, 2017, www.huffingtonpost.de/2017/01/04/de-maiziere-konzept-sichere_n_13947896.html(link is external).
- [38] “Reform der Sicherheitsbehörden – Wie wär’s mit einem deutschen FBI?” *Spiegel Online*, August 22, 2017, <http://www.spiegel.de/panorama/justiz/sicherheit-in-deutschland-wie-waer-s-mit-einem-deutschen-fbi-a-1162781.html>(link is external).
- [39] The press release of the German government about the implementation and benefits of the statute is available at www.bundesregierung.de/Content/DE/Artikel/2015/12/2015-12-09-datenaustauschverbesserungsgesetz-fluechtlingsausweis.html(link is external).
- [40] The press release of the German federal police about the implementation of the RADAR-iTE system is available at <https://www.bka.de/DE/Presse/Listenseite> (link is external) *Pressemitteilungen/2017/Presse2017/170202_Radar.html*.

[41] "Rückführung von Flüchtlingen – Deutschland und Tunesien starten Pilotprojekt für Abschiebungen," *focus online*, March 1, 2017, <http://www.focus.de/politik/ausland/migration-auch-tunesien-kooperiert-bei-abschiebungen-aus-deutschland> (link is external) id_5326677.html.

[42] These topics are ongoing subjects of the political debate in the different committees on internal affairs. Different legislative and resolution proposals are currently discussed, such as the proposal to implement a nationwide prevention strategy against radicalization as proposed by the Party Bündnis 90/ die Grünen: <http://dip21.bundestag.de/dip21/btd/18/104/1810477.pdf>(link is external).

[43] As quoted in Matthew Karnitschnig, "Terror sparks call to centralize German police powers," *Politico*, January 3rd, 2017, <http://www.politico.eu/article/terror-sparks-call-to-centralize-german-police-powers-berlin-isil-security>(link is external).

Presenting a Strategic Model to Understand Spillover Effects of ISIS Terrorism

Cüneyt Gürer

Abstract:

Understanding the nature and the extent of the future threat from ISIS has been a key question for scholars, policy makers and security professionals since ISIS started losing significant grounds in Syria and Iraq. This article analyses ISIS terrorism and its possible spillover effects from a regional security perspective by presenting a strategic model to develop options for the policy makers. A strategic understanding, supported by a model that has been designed to capture all possible variables and their interaction which each other, is necessary to understand the future direction of the threat. Many scholars agree that the threat is not only about the organizational structure of ISIS but also its ideological aspect, therefore the model presented here connects the facts and the ideology with variables at three different levels: regional political level; ISIS and its organizational structure; and individual level variables. The model was designed to capture changes with relevant data thus providing a strategic data-driven understanding of the threat. Regional political developments and how ISIS reacts to those developments are the main concerns at the first two levels of analysis. Foreign fighters and other sympathizers are the most important subjects of the study at the individual level with the assumption that the future threat will diffuse through foreign fighters and self-radicalized lone actors.

Introduction

ISIS poses a significant threat to both Middle East and global security. Studies analyzing the organizational structure, recruitment process, target selection and attacks of ISIS by focusing its leaders and followers' public and social media discourses found that the organization developed a decentralized attack strategy by encouraging its sympathizers for the attacks and not addressing direct attack plots.^[1] Attacks carried out by ISIS affiliated militants in 2015, 2016 and 2017 indicate that the organization is becoming a more global threat. Although recently ISIS lost significant grounds both in Syria and Iraq, its last stronghold places to be expected to fall soon, there is also convincing evidence that ISIS adapts to these changes.^[2] The loss of territory was followed by loss of manpower as many foreign fighters escaped from Syria and started to return to their home countries or to a third country, continuing however to keep their contacts with the organization.^[3]

Mostly operating in Syria and Iraq and establishing a governance structure in Syria, ISIS received a significant number of foreign fighters in the past. ISIS not only created a regional insecurity and instability but also spread the terror to a global level through foreign fighters and other radical individuals called "lone actors." Returning foreign fighters are already involved in terrorist attacks, particularly in Europe, and current indications demonstrate that returnees and lone actors will continue to pose significant threat to the global security.

This article analyzes ISIS terrorism and its possible spillover effects from a regional security perspective and attempts to present a model for developing alternative directions for the policy makers. In order to make an accurate analysis, it argues that three types of data should be collected and cross-analyzed to measure the causal relationship at different levels. The model created to understand the spillover effect of ISIS terrorism starts with the regional level events (*regional level analysis*) and continues with the policy outcomes of regional actors. At the second step, an organizational level approach focusing on ISIS (as a non-state actor) attempts to develop an understanding of the organization. Lastly, the study argues that individual level data collection focusing directly on key individuals and known foreign fighters as well as individuals at risk will be necessary to predict the nature and the extent of the spillover effect of ISIS terrorism.

Security at the Global Level in 2016 and 2017

ISIS carried out or claimed responsibility of more than 140 terrorist attacks in 30 countries other than Iraq and Syria since declaring its self-proclaimed Islamic State (the caliphate), i.e. from June 2014 until the first two months of 2017.[4] According to the Esri Story Map project data, until September 4, 2017 133 attacks were carried out at the global level killing more than 800 people (excluding Iraq and Syria).[5] Those attacks taking place from North America to Australia and Europe to South Asia clearly show that since 2014 ISIS became a more global threat than a regional one (See Figure 1 and Figure 2). Although most of the attacks (including the ones with most casualties) were carried out in the Middle East and North Africa (MENA), the return of foreign fighters increases the concerns for the global security in the Western world. Recent attacks in 2016 and 2017 require experts and policy makers to develop a better understanding of the spillover effect of ISIS terrorism at the global level.

Available data regarding the terrorist attacks and public perception of safety and security presents an interesting paradox. According to the 2017 Global Peace Index Report, MENA region ranks the least peaceful region in the world for the fifth successive year and Europe remains the most peaceful region in the world, with eight of the ten most peaceful countries coming from this region.[6] On the other hand, Special Eurobarometer Survey on Europeans' Attitudes toward Security indicates that, although Europe remains the most peaceful region in the world, most of the Europeans rank terrorism as the most important threat (49%) to the security of EU citizens and their feeling of security deteriorating.[7]



Source: CNN International, "Mapping ISIS attacks around the World" (Sanchez et al, 2016).

Figure 1: ISIS Attacks at the Global Level 2016.

Respondents to the survey believe that many of the security threats the world faces are becoming more severe; two-thirds of respondents (68%) think that the challenge of terrorism is likely to increase over the next three years (up from 51% in 2011), whereas only 10% believe it is likely to decrease. Security data showing that a region is safe does not mean that the public fully enjoys the level of security demonstrated in the data. Public perception of the security and fear of victimization as well as increasing concerns for the possibility of attacks determines the actual demand for more effective security policies. In other words, in Europe, there is a demand not only *to be safe* but also—and may be, more importantly—*to feel safe*.

The attacks in Paris in November 2015 have been marked as the worst violence (130 killed and 368 wounded) in France since WWII and "the most sophisticated assault in the West." [8] After the attacks many experts and

commentators claimed that the world entered a new area of counter terrorism and the Paris attack became a game changer for the West as well as at the regional and transnational security domain. The San Bernardino attack in the US in December 2015 that resulted in 14 dead and 24 injured increased the attention to the capacity of ISIS to conduct remote attacks even without sending direct orders for an attack plot. In 2016, ISIS claimed responsibility for 16 deadly attacks in the West (in the US, France, Belgium, Turkey, Germany) killing 302 and wounding 1277. Until September 2017 ISIS carried out (or inspired) six major attacks (in the UK, France, Turkey, and Spain) and killed 91 and wounded 327.[9] According to latest Europol report, majority of attacks claimed by ISIS in Europe are masterminded and perpetrated by individuals inspired by ISIS and the organizational structure of ISIS played no or very limited direct role in planning and executing the attacks.[10] According to the same report, the number of arrests for jihadi terrorists activities has increased dramatically in the EU during the last few years with more than 600 arrests in 2015 (395 in 2014, 687 in 2015) and also the number of plots by jihadi terrorists have never been as high as in the period 2014-2016. Europol concludes that there is an IS-effect on jihadi terrorism in Europe from the turn on 2013.

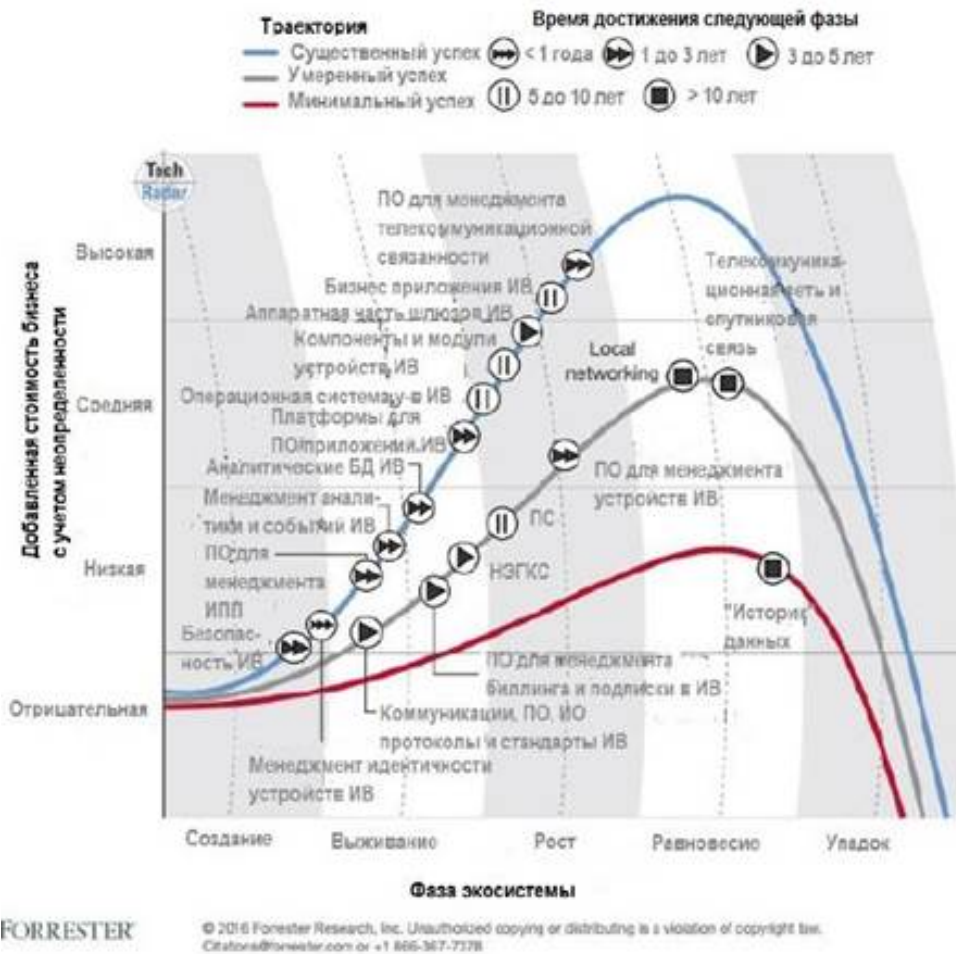
Available data on ISIS attacks at the global level indicates that inspired attacks by people who have previously travelled to Syria and trained by ISIS pose a significant risk for States receiving those individuals. A recent report by Swedish Defense University points out a risk that “some of the returning foreign fighters intend or can be swayed to commit attacks in Sweden and other countries outside of the conflict area, and at least two Swedish returnees were involved in the recent Paris and Brussels attacks.”[11]

Investigations of some of the attacks between 2015 and 2017 revealed that some of the attackers had traveled to Syria and trained by ISIS before the attacks. In July 2015, a 20-year-old suicide bomber with links to ISIS killed more than 30 people at the Cultural Center in Suruc, Southeast part of Turkey and very close to the border with Syria.[12] Investigations after the November 2015 Paris attacks (130 death and 368 wounded) also found individuals who were returnees from Syria to be involved in the attack.[13] On January 12, 2016 a suicide bomber killed 10 people and wounded 15 at Sultanahmet square, a popular tourist district in Istanbul. The attacker, Nabil Fadli, a Syrian born in 1988, was later identified as a registered Syrian refugee, affiliated with ISIS before his travel to Turkey.[14] On March 22, 2016 three coordinated attacks killed 35 and wounded 340 people in Brussels and at least two of the suspects had previously travelled to Syria and fought for ISIS.[15] Further analysis of similar cases shows that individuals who have been recruited by ISIS and traveled to Syria started to engage in terrorist acts in close cooperation with individuals who never traveled but were radicalized in their home countries. Therefore, there are significant indications that returnees started to be the agents of spillover between 2015 and 2017. Some of the attacks however carried out by lone actors and self-radicalized individuals, therefore these two phenomena (interaction of returnees and lone actors) needs to be carefully examined in order to reach reliable conclusions as to the future direction of the threat.

Security and related issues are also listed amongst the most discussed topics in 2015. Facebook analyzed and revealed its data on conversations at the global level and found that November 13 Paris attacks took the second place after US presidential election.[16] Other related topics such as “Syrian civil war and refugee crises” took the third place, “fight against ISIS” became the seventh, and “Charlie Hebdo attack” listed eighth most talked-about topics at the global level in 2015. When you compare the same data with 2014, only “conflict in Gaza,” as a security related topic, appeared in the list as the sixth talked about topic (Table 1). Interestingly, in 2016 none of these issues were in the Facebook’s top ten most talked global topics.[17] However, a recent Pew Research Center data shows that ISIS is still considered as the top threat at the global level.[18]

These two data sources and the Eurobarometer survey mentioned earlier illustrate that although people stop talking about the security related issues overtime, how they conceive threat and their threat perceptions do not change significantly. Security related issues and concerns became a significant part of our daily lives, an important determinant of our personal and professional choices, have a direct impact on our social and political behaviors. Therefore, addressing the complex security problem of the day requires a multi-dimensional and more complex methodological analysis. Descriptive findings are mostly irrelevant to the development of comprehensive policy solutions based of understanding of the future direction of the threat. By providing a framework and a model this study intends to create a scientific analysis tool to measure possible spillover of ISIS terrorism.

Security concerns and related issues have been related to several major issues in the Middle East such as the Israel-Arab conflict, developments followed by the Arab Spring, Syrian civil war, etc. All those issues have deep historical and political backgrounds and almost turned into *frozen policy areas*, which produce no long-term solutions. Most of these conflicts and issues are also blamed for being the root causes of recently emerging security threats and the birth of ISIS itself. ISIS emerged in 2006 from the remnants of Al-Qaeda in Iraq after the American invasion; the group became internationally known after expanding to Syria in 2013 and declaring global Caliphate (Global Islamic State) in 2014.[19] As ISIS becomes weaker in Syria and Iraq, there are indications that the ideology and frozen policy issues that radical groups rely on for their existence will remain in the future. Therefore it is likely that the threat will appear with a new face; hence, the international security community needs to focus on the re-emergence of the threat with different structure, new actors and diverse modus operandi by considering all relevant aspects in a single comprehensive model. This study is an attempt to create an effective tool to examine multiple aspects of the issue with account of their interaction.



Source: Esri Story Map 2017 Terrorist Attacks.

Figure 2: ISIS Attacks at the Global Level 2017.

Table 1. Top Global Topics in 2014, 2015 and 2016.

	Top Global Topics of 2014	Top Global Topics of 2015	Top Global Topics of 2016
1.	World Cup	US Presidential Election	US Presidential Election
2.	Ebola virus outbreak	November 13 Attacks in Paris	Brazilian Politics
3.	Elections in Brazil	Syrian Civil War & Refugee Crisis	Pokemon Go
4.	Robin Williams	Nepal Earthquakes	Black Lives Matter
5.	Ice Bucket Challenge	Greek Debt Crisis	Rodrigo Duterte & Philippine Presidential Election
6.	Conflict in Gaza	Marriage Equality	Olympics
7.	Malaysia Airlines	Fight Against ISIS	Brexit
8.	Super Bowl	Charlie Hebdo Attack	Super Bowl
9.	Michael Brown/Ferguson	Baltimore Protests	David Bowie
10.	Sochi Winter Olympics	Charleston Shooting & Flag Debate	Muhammad Ali

Source: Data from Facebook Newsroom: 2014, 2015 and 2016 Year in Review.

ISIS and Security in the Middle East: Introduction to the Spillover Model

Despite other frozen policy issues in the Middle East, security politics progress over the years and most of the changes are related to global, regional and domestic developments. Not all changes produce positive results all the time but as the countries reach an agreement on regional problems and develop a working cooperation environment, promising results obtained in countering threats and further achievements become more likely. In addition to the development of a common response to the ISIS threat, a multi-disciplinary approach should also be developed and regional policies have to be analyzed with account of the interplay of all possible causes and effects, since policy outcomes and negative externalities (such as terrorist attacks) do happen in connection with internal and external factors.

Cascade Path Model to Measure Spillover

Understanding the spillover effect of ISIS terrorism requires creating a model to capture all changes (both internal and external) at three different levels to understand the direct or indirect causal relationships amongst various variables. The model presented in Figure 3 shows a cascade model (assuming each component has an independent impact on each other) and six paths showing the possible interaction between three different levels. These levels were identified on the basis of a theoretical understanding of the spillover model, in which regional politics and ISIS, a non-state actor, interact with each other (that interaction produces negative externalities) whereas foreign fighters are presented as the agents of the spillover in the same model.[20]

According to the model, all these levels have direct and indirect impacts on regional security. The model will help us break down the complex issue where focusing on each path will contribute to understanding the power of each interaction and, hence, developing new policy alternatives. This model is also intended to be used as a framework for developing a data collection instrument to create a database for further analysis.

Component 1: The first component of the model focuses on regional politics and proposes the collection of regional level data and it involves following major events and policy changes of regional actors. Path 1 (P1) refers to one-way causal relationship between regional politics and ISIS; it shows how regional politics will affect the ISIS (its policies, organizational structure, leadership etc.). P2 refers to how regional politics might have a direct impact on individual level data such as foreign terrorist fighter (FTF) recruitment, constructing new individual level narratives, etc.

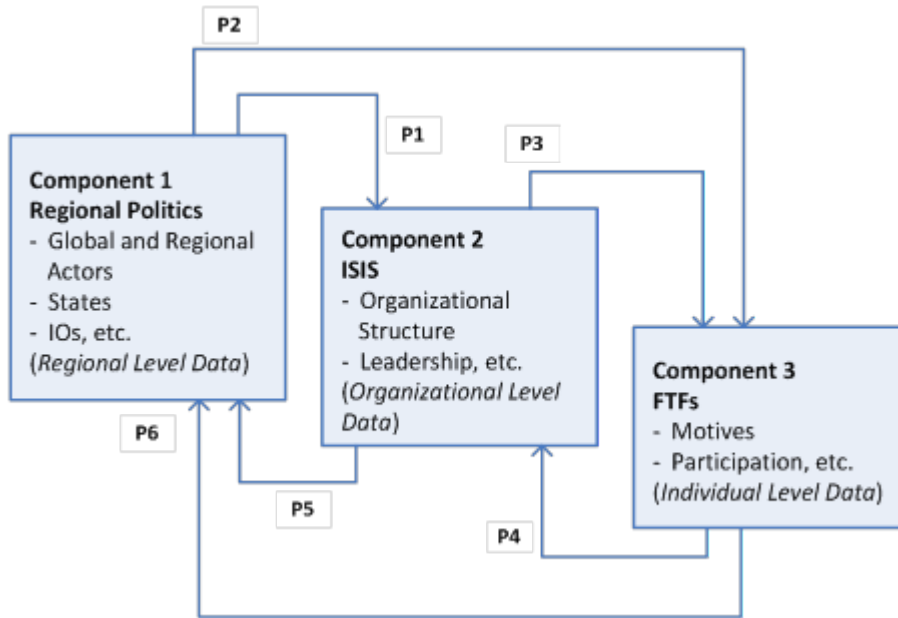


Figure 3: ISIS Attacks at the Global Level 2017.

Component 2: As the first component of the model focuses more on regional and state level analysis, the second component focuses on institutional level analysis and is intended to analyze ISIS from an organizational point of view. Changes in the organizational structure, developing new or adaptation of existing discourses and ways of countering actions undertaken by international coalition or individual states’ policies are all examined at this level. In this component, it is also intended to follow ISIS from an analytic perspective and identify changes in the organizational structure, method of governance and management style based on P1 and P4. This component also has two outgoing paths and P3 refers to the effect of ISIS on FTFs and P5 – on how ISIS creates an impact on regional policies.

Component 3: In the last component, the model seeks to collect data at the individual level. It includes variables to identify the patterns and characteristics of FTFs at the global level. In this component, the intention is to collect data from open sources about the individuals who are prone to or have already joined ISIS and to try to understand the dynamics of involving the organization and power of narratives. In the path structure of the model, P4 stands for the possible effects of individuals on the organization and P6 refers to FTFs’ possible effects on changing regional politics or a specific policy.

Applying the Model to 2015 and 2016

Changes in world politics do not happen overnight. Although some single events create enormous impacts in a shorter time period, in most cases significant change comes upon certain preconditions or as a result of the influence of direct/indirect causes. Regional political and policy level changes play an important role to understand the security structure of a region. From the perspective of the model created in this study, these changes have a significant impact on the lower levels (to ISIS and FFs). In other words, regional changes will have an impact both on the variables related to ISIS as an organization and to the FFs.

Scholars focusing on regional studies and in particular on the Middle East mostly agree with the argument that the region is suffering from the lack of regional integration and linkages necessary to enter the global world.[21] Theories of international and comparative politics provide many explanations why the region does not have a stable regional system and why states in the region cannot develop regimes that contribute to peace and an inclusive economic prosperity.

Comparing the Middle East with other regions also provides an explanation why the Middle East could not establish a stable regional system. Etel Solingen, after conducting a comparative analysis between East Asia and the Middle East, claims that those two regions developed a divergent development path over the last century

despite their initially shared conditions.[22] She concludes that competing models of political survival explain the difference in economic, political and regional developmental difference, while “East Asian leaders pivoted their political control on economic performance and integration in the global economy whereas Middle East leaders relied on inward-looking self-sufficiency, state and military entrepreneurship and a related brand of nationalism.”

The Middle East as a regional entity does not have much power and influence hence almost zero ability for establishing a security policy to mobilize regional states. The lack of a powerful regional institutional structure and limited abilities of regional states to create a well-functioning security structure leaves a wide area for global actors to interfere and define regional policies. Therefore, the Middle East remains referring only to a geographical entity rather than a political, economic, cultural or a military structure. Hence, it would be a fair argument to claim that there is no structure in the region to bring peace and stability. Main actors in the regional politics are states (both internal and external but external states have more influence), international organizations (both regional and global institutions, with the later having more power) and non-state actors (global level NGOs mostly providing positive impact and terrorist organizations having negative impact on the regional security.)

According to Curtis R. Ryan, regime security is the key driver of alliance politics in the Middle East and succinctly explains the international relations of the region.[23] That is, Arab states are concerned over their regimes as political developments emerge in the region. Ryan claims that “Arab regimes remain frequently trapped in an internal and external security dilemma of their own making and obsessed with ensuring the security of their ruling regimes against both internal and external challenges. In sum, we can argue that the Middle East international relations are shaped and defined by an interplay between domestic and regional influences.”[24]

In 2015 and 2016, the MENA did not progress; not even a single step was made towards constructive institutional cooperation. As presented earlier in this study, security problems in the region became more global and earlier complications became more complex. 2015 started with an ongoing war between Kurdish forces of People’s Protection Units (YPG) and ISIS militants in Northern Syria over Kobani (Syrian city close to Turkish border.) After 113 days of war between the two groups, YPG won the battle and re-captured the city from ISIS on January 27, 2015. Within Syria, the pattern of fighting from the previous years continued, sectarian and ethnic differences started to drive clashes, and power has shifted from large standing armies to local militias in 2015.[25]

Among others, one significant event of 2015 was the changed Russian approach to the Syrian problem. More specifically, during the UN General Assembly meeting on September 28, Russia clearly showed a significant shift followed by Russian airstrikes on ISIS targets in Syria on October 1, 2015. New developments in 2015 clearly showed that Russia as an active actor and participant in the regional politics changes the way the Syrian crises is and can be handled. However, that shift neither significantly contributed to the security of the region nor made any changes in the power structure. ISIS also continued to hold on to most of its territory, or even expand it, established a government bureaucracy, and recruited new fighters from all over the world.

Measuring the effect of regional developments on the organizational side of ISIS is the key objective of the first component of the model. Available data suggests that regional developments had limited impact on diminishing the power of ISIS at the global level. Both in 2016 and 2017 Western coalition forces, with significant involvement of local opposition and militia groups, advanced to gain territories previously claimed by ISIS in Syria and Iraq, however this battle is not over yet. Military experts expect to claim a full-scale victory by retaking Raqqa (the so called capital of the Islamic State) before the end of 2017. Despite this military defeat, in 2016 ISIS either directly organized or claimed responsibility of many deadly attacks carried out by returnees or self-radicalized individuals. As Daniel Byman, senior fellow at Brookings Institution, puts it, in 2016 and 2017 ISIS showed its ability to conduct attacks at the global level other than the conflict area.[26] What to expect after a military victory in Syria and how to deal with the potential of ISIS to conduct attacks at the global level has been and will be a major issue for the following months and the ideology will be the major tool for the organizational structure to recruit members for potential attacks.[27]

The structure and the ideology of ISIS developed within the context of the Iraqi insurgency of the early 2000s. It began as a branch of Al-Qaeda, founded in Iraq in 2004 after the American invasion and headed by Ayman

al-Zawahiri and mostly shaped by Abu Mus'ab al-Zarqawi until he was killed by U.S. airstrikes in Iraq.[28] In October 2006, Abu 'Umar al-Baghdadi has been named as the leader of the group by the Mujahidin Shura Council in Iraq. Between 2006 and 2013, the group named itself as the Islamic State of Iraq (ISI) and mostly considered as Al-Qaeda in Iraq by the Western media. In April 2013, Abu 'Umar al-Baghdadi announced the Islamic State's expansion to Sham, the Arabic word for greater Syria. On June 2014, ISIS declared itself the caliphate and Baghdadi announced himself as the caliph of all Muslims throughout the world.

At every stage of its development, ISIS constructed a governance structure including management of educational, judicial, security, humanitarian and infrastructure systems. Caris and Reynolds, based on the available data and evidence, explain in detail how ISIS has demonstrated the capacity to govern both rural and urban areas in Syria under its control.[29] With its weaknesses and strengths, ISIS developed administrative capacities in Syria, and in order to understand the operation strategies of the organization that structure should be carefully examined. Available data do not support the suggestion that the organizational structure of ISIS changed in 2015 and there is not much evidence to measure how military advancements in 2016 changed the organizational structure of ISIS.

Addressing the return of foreign fighters became a high priority for Western countries and recently foreign fighters have been the subjects of important debates. Although the term foreign fighters had been used for a long time, recently it has been mostly used in reference to people who travelled to Syria and Iraq to join ISIS and other terrorist organizations. Many conflicts in the world received people who have volunteered to fight for their cause, and we can find examples of this in Afghanistan during Russian invasion, in Balkan conflict and as well as in the more recent Ukraine-Russia conflict over Crimea. This phenomenon is not specific to a group of people, to a religion or a nation. However, the scale of the threat is immense due to direct influences of technological advances as well as the outbreak of civil war and sectarian violence in several countries in the Middle East.

The Soufan Group released a report in June 2014 presenting the known numbers and other available background information on Foreign Fighters in Syria identifying approximately 12,000 foreign fighters from 81 countries.[30] In a later report, released in December 2015, it is indicated that "despite the sustained international effort to contain the Islamic State and stem the flow of militants traveling to Syria, the number of foreign fighters have more than doubled." [31] The same report also presents that "between 27,000 and 31,000 people from at least 86 countries have traveled to Syria and Iraq to join the Islamic State and other violent extremist groups, and efforts to contain the flow of foreign recruits to extremist groups in Syria and Iraq have had limited impact. The most worrisome fact for the European countries is that "the number of foreign fighters from Western Europe has more than doubled since June 2014, and the average rate of returnees to Western countries is now at around 20-30%, presenting a significant challenge to security and law enforcement agencies that must assess the threat they pose." In 2015, a significant number of foreign fighters continued to join ISIS and some of them returned back to their home countries. Not all of them engaged in a terrorist activity but the risk for home countries is very high.

Analysis and Conclusion

In order to understand the spillover effect of ISIS terrorism three components—regional politics, ISIS, and foreign fighters—were presented and assumed to have an independent impact on each other in this paper. Therefore, the model consisted of direct relationship amongst all these components. Available data supported some of the theorized connections but for more comprehensive results longer term data collection and its analysis is required and that is beyond the limits of this study. Since the main purpose of this study is to present the model and suggest an ongoing data collection activity to create a database for an extensive analysis, it suffices to make some general conclusion with the available data.

Our model indicates that regional political developments in the Middle East do not promise a comprehensive institutionalized cooperation environment. In addition, regional political developments and changes in policies in 2015 did not cause significant damage to ISIS, nonetheless Western coalition forces made significant progress to defeat ISIS in Iraq and Syria by re-taking the claimed territory. Meservey reported that ISIS lost 14% of its claimed territory in 2015, but how that effected the organization and its power structure is unclear.[32] The long-term impact of current military success is not clear yet and requires further political and social successes both at

the regional and global level. Whether or not regional actors' specific policies create any type of impact on the organization requires the collection of more data. Path 1 (P1) in our model presented earlier in Figure 3 shows no significant impact on ISIS to reduce its power in 2015.

In 2015, regional key actors could not develop an advanced cooperation to reduce participation to ISIS. However, increase in the level of intelligence sharing and more cooperation at the technical level produced promising results in comparison to previous years. If regional political shift can put ISIS in a difficult position that it cannot survive, it would also lose control over the members and foreign fighters would seek opportunities to flee from Syria or Iraq. However, until 2015, there was no indication of such development which happened later in 2016 and 2017. Therefore, P2 in our model indicated limited but still promising outcomes in 2016 and 2017.

In order to measure the impact of ISIS on FTFs (P3), the measurement should include variables about individuals who already joined the group and characteristics of potential FTFs abroad. Statements of people who managed to escape from ISIS indicate that the organization is not as they were expecting to be.[33] More data is required to make a clear assessment regarding ISIS and FTFs interaction. Until 2016 and also in 2017, available data indicates that ISIS created a strong organization structure using social media effectively and also managing all recruits effectively as they join their forces.

Key players in the regional politics established a coalition to counter ISIS's territorial expansion, but the real impact on the organization is not sufficiently clear to reach a conclusion of a final defeat of ISIS. ISIS still holds the advantage of using global sympathizers and former fighters who returned to their home countries as the agents of spillover. Regional politics cannot be successful unless all components of the problem are addressed and the interaction amongst them is assessed cautiously. Scholars should go beyond the descriptive studies and produce more policy options for decision makers by mostly addressing the individual level push and pull factors to reduce ISIS's advantage to recruit more people to be employed in future attacks. Military and law enforcement solutions will be effective only if States and international organizations increase their tactical level cooperation and extend this cooperation to a more strategic level by understanding each individual component and the interaction among components thoroughly. The strategic model presented in this study will provide analytical information that will help policy makers to identify the issues requiring more attention and also will produce information to address possible vulnerabilities emerging after new political or social developments.

After defeating ISIS in Syria and Iraq, a new era of fight will start that will include greater focus on ideology, methods used to recruit new members, and efforts to reduce the likelihood of individuals conducting lone actor attacks. A short term tactical solution will include more international cooperation and sharing data on the returnees and possible radicalized individuals as well as members of the group. Another more strategic level approach requires close understanding of the background factors triggering radicalization of individuals and how national and international political developments feed this circle. Each component will only be valuable if the interaction of global, national and individual factors leading to violent attacks could be better understood. A more effective strategy to defeat ISIS and to reduce capacity to attack at the global level depends on a multi-disciplinary understanding of the spillover and developing multi-sectoral policy responses to the future threat of ISIS.

About the author

Dr. Cüneyt Gürer is Associate Professor of Security Studies. He is an Adjunct Faculty Member of George C. Marshall European Center for Security Studies. His research interest are global and regional security policies, methodological approaches to security and policy diffusion. He earned his PhD from Kent State University Department of Political Science in 2007.

-
- [1] Thomas Hegghammer and Petter Nesser, "Assessing the Islamic State's Commitment to Attacking the West," *Perspectives on Terrorism* 9, no. 4 (August 2015): 14–30; Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (December 2014): 1–22.
- [2] "Syria: ISIS to be driven out of Raqqa within two months, claims top commander," *Independent*, August 28, 2017, <http://www.independent.co.uk/news/world/middle-east/isis-driven-out-of-raqqa-syria-two-months-ypg-nowruz-ahmed-a7917326.html>(link is external) (accessed September 6, 2017).
- [3] "ISIS faces exodus of foreign fighters as its 'caliphate' crumbles," *The Guardian*, April 26, 2017, <https://www.theguardian.com/world/2017/apr/26/isis-exodus-foreign-fighters-caliphate-crumbles>(link is external) (accessed September 6, 2017).
- [4] For the global level data and other information on attacks see Ray Sanchez, Tim Lister, Mark Bixler, Sean O'Key, Michael Hogenmiller, and Mohammed Tawfeeq, "ISIS goes global: 143 attacks in 29 countries have killed about 2,043 people," *CNN International Edition*, January 21, 2016, <http://edition.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world>(link is external) (accessed September 7, 2017).
- [5] "Esri Story Map 2017 Terrorist Attacks," <https://storymaps.esri.com/stories/terrorist-attacks/?year=2017>(link is external) (accessed September 7, 2017). The data derived from the web site and calculated manually by the author to exclude cases from Syria and Iraq.
- [6] Institute for Economics and Peace, "Global Peace Index 2017 Measuring Peace in a Complex World," <http://visionofhumanity.org/app/uploads/2017/06/GPI17-Report.pdf>(link is external) (accessed September 7, 2017).
- [7] European Commission Public Opinion, "Special Eurobarometer 432, Europeans' Attitudes Towards Security," <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/search/security/surveyKy/2085>(link is external) (accessed September 7, 2017).
- [8] Emily Estelle and Harleen Gambhir with Kaitlynn Menoche, "Network Graph of ISIS's Claimed Attack in Paris" (Institute for the Study of the War, 15 November 2015), <http://www.understandingwar.org/backgrounder/network-graph-isis-claimed-attack-paris>(link is external) (accessed September 7, 2017).
- [9] "Esri Story Map 2017 Terrorist Attacks." The data derived from the website and calculated manually by the author.
- [10] "Changes in Modus Operandi of Islamic State (IS) revisited," European Union Terrorism Situation and Trend Report (Europol, 2017), <https://www.europol.europa.eu/newsroom/news/2017-eu-terrorism-report-142-failed-foiled-and-completed-attacks-1002-arrests-and-14...>(link is external) (accessed September 7, 2017).
- [11] Linus Gustafsson and Magnus Ranstorp, *Swedish Foreign Fighters in Syria and Iraq: An analysis of open-source intelligence and statistical data* (Swedish Defence University: Center for Asymmetric Threat Studies (CATS), 2017), <http://fhs.diva-portal.org/smash/get/diva2:1110355/FULLTEXT01.pdf>(link is external) (accessed September 7, 2017).
- [12] "Suruc massacre: 'Turkish student' was suicide bomber," *BBC News*, July 22, 2015, <http://www.bbc.com/news/world-europe-33619043>(link is external) (accessed September 8, 2017).
- [13] "Hollande says Paris attacks an 'act of war' by Islamic State group," *France 24*, November 15, 2015, www.france24.com/en/20151114-paris-attacks-president-hollande-act-war-islamic-state-group-terrorism-france(link is external) (accessed September 8, 2017).
- [14] Ceylan Yeginsu and Victor Homola, "Istanbul Bomber Entered as a Refugee, Turks Say," *The New York Times*, January 13, 2016, <https://www.nytimes.com/2016/01/14/world/europe/istanbul-explosion.html>(link is external) (accessed September 8, 2017).
- [15] "ISIS supporters claim group responsible for Brussels attacks: 'We have come to you with slaughter'," *Independent*, March 22, 2016, <https://www.independent.co.uk/news/world/europe/isis-supporters-claim-responsibility-for-brussels-attacks-bombings-belgium-airpo...>(link is external) (accessed September 8, 2017).
- [16] "2015 Year in Review," *Facebook Newsroom*, December 9, 2015, <http://newsroom.fb.com/news/2015/12/2015-year-in-review/>(link is external) (accessed January 24, 2016).
- [17] "Facebook's 2016 Year in Review," *Facebook Newsroom*, December 8, 2016, <https://newsroom.fb.com/news/2016/12/facebook-2016-year-in-review/>(link is external) (accessed September 8, 2017).
- [18] Jacob Poushter and Dorothy Manevich, "Globally, People Point to ISIS and Climate Change as Leading Security Threats" (Pew Research Center, 1 August 2017), <http://www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/>(link is external) (accessed September 5, 2017).

- [19] Cole Bunzel, *From Paper State to Caliphate: The Ideology of the Islamic State*, The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper No. 19, (Brookings: Center for Middle East Policy, March 2015), <https://www.brookings.edu/wp-content/uploads/2016/06/The-ideology-of-the-Islamic-State.pdf>(link is external) (accessed September 8, 2017).
- [20] Spillover might be also caused by other variables such as terrorist narratives, social media images and discussions created by other entities other than the ISIS. However, this model assumes FFs as the key spillover agents and pays special attention to them.
- [21] Jerry W. Wright and Laura Drake, eds., *Economic and Political Impediments to Middle East Peace: Critical Questions and Alternative Scenarios* (New York: Palgrave Macmillian, 2000).
- [22] Etel Solingen, "Transcending disciplinary divide/s," in *International Relations Theory and a Changing Middle East*, Project on Middle East Political Science Studies, September 17, 2015, <http://pomeps.org/2015/09/17/international-relations-theory-and-a-new-middle-east/>(link is external) (accessed November 1, 2015).
- [23] Curtis R. Ryan, "Regime Security and Shifting Alliances in the Middle East," in *International Relations Theory and a Changing Middle East, POMEPS Studies* 16 (Aarhus University, September 2015), 42-46.
- [24] Bassel F. Salloukh, *Syria and Lebanon: A Brotherhood Transformed*, Middle East Report No. 236 (Middle East Research and Information Project, 2005), <http://www.merip.org/mer/mer236/syria-lebanon-brotherhood-transformed>(link is external) (accessed September 8, 2017).
- [25] Brian Michael Jenkins, *How the Current Conflicts Are Shaping the Future of Syria and Iraq* (Santa Monica, CA: RAND Corporation, 2015), <http://www.rand.org/pubs/perspectives/PE163.html>(link is external) (accessed September 8, 2015.)
- [26] Daniel Byman, "Beyond Iraq and Syria: ISIS' ability to conduct attacks abroad," *Brookings*, June 8, 2017, <https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/>(link is external) (accessed September 8, 2017).
- [27] I am aware of the fact that this type of conclusion will be more accurate after analyzing extensive data and examining key political security developments and their impacts on subsequent events. However, considering the space limitations for this article, a short and rough analysis for 2015 and 2016 is provided.
- [28] Bunzel, *From Paper State to Caliphate: The Ideology of the Islamic State*, 13.
- [29] Charles C. Caris and Samuel Reynolds, *ISIS Governance in Syria*, Middle East Security Report 22 (Washington, D.C.: Institute for the Study of War, July 2014), http://www.understandingwar.org/sites/default/files/ISIS_Governance.pdf(link is external) (accessed September 7, 2017)
- [30] Richard Barrett, *Foreign Fighters in Syria* (New York: The Soufan Group, June 2014), <http://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdf>(link is external) (accessed November 23, 2016).
- [31] *Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq* (New York: The Soufan Group, December 2015), http://soufangroup.com/wpcontent/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf(link is external) (accessed January 23, 2016).
- [32] Joshua Meservey, "Al Shabab's Lessons for ISIS: What the Fight Against the Somali Group Means for the Middle East," *Foreign Affairs*, January 24, 2016, <https://www.foreignaffairs.com/articles/ethiopia/2016-01-24/al-shababs-lessons-isis>(link is external)(accessed January 26, 2016).
- [33] Anne Speckhard and Ahmet S. Yayla, "Eyewitness Accounts from Recent Defectors from Islamic State: Why They Joined, What They Saw, Why They Quit," *Perspectives on Terrorism* 9, no. 6 (December 2015): 95-118.

Facing an Unpredictable Threat: Is NATO Ideally Placed to Manage Climate Change as a Non-Traditional Threat Multiplier?

Amar Causevic

Abstract:

This paper examines NATO's perception of climate change as a non-traditional threat multiplier. For well over a decade, European as well as Pentagon and other U.S. government studies and policy documents have noted that as the planet continues to warm, arable land continues to disappear, cyclones become more powerful, droughts increase in impact, food shortages are more frequent, and thousands of climate migrants are on the move. All of these climate change-related factors significantly increase the likelihood of conflict escalation. The threat multiplier characteristic of climate change will only exacerbate problems such as government instability, the spread of disease, conflicts over water supplies, the strengthening of terrorism, and widespread migration. This research explores NATO's initiatives to deal with this non-traditional threat multiplier and analyzes how different schools of international relations theory define climate change and address this security concern. In addition, the article provides insights into how climate change-induced threats affect the socio-economic and political security of nation states and what that means for NATO. Finally, the research provides a review of the Alliance's engagement, policy frameworks, operations, and units re-sponsible for tackling threats originating from climate change. It concludes with the recommendation that NATO has made significant progress on placing climate change on its threat radar, but that the Alliance will have to do more to integrate these concerns because current efforts are not sufficient to meet future security challenges stimulated by increase in the average global temperature.

Introduction

Climate change represents a non-traditional threat to international security and the future existence of modern civilization. Year after year, drought, famine, storms, and flooding become more and more frequent and destructive. Besides being a non-traditional threat, climate change impacts are a threat multiplier. Multiplier effects of climate change are reflected in a worsened ability for families to provide for themselves, increasing refugee and migration flows, and may even act as a catalyst for the spread of diseases, potentially causing or exacerbating lethal pandemics. Increased occurrence of extreme weather patterns and major natural disasters amplify the risk of and result in significant population displacement.^[1] Increased temperatures and the resulting negative effects will not bypass military operations, personnel, and installations. For example, sea level rise and increased incidence of hurricanes will directly affect military facilities, increase the cost of security, and impede states' and alliances' capacity to address traditional threats.^[2]

The North Atlantic Treaty Organization (NATO) is the biggest and most powerful military alliance in the world. Its main responsibility is to provide security for North America and its European member states; however the Alliance has long been directly and indirectly engaged in providing security to non-NATO member states. Ever since the September 11 attacks, NATO has taken on a range of non-traditional military roles such as assisting in counter-piracy operations, enforcing no-fly zones, peacekeeping, working with various multilateral organizations on institution-building in fragile states, providing humanitarian assistance, etc.

This article addresses the following research question: To what extent is NATO capable of managing climate change as a non-traditional threat multiplier? First, the essay examines the theory of realism and its perception of threat. This theoretical framework was chosen because NATO is an organization that originated in the Cold War, during which realist philosophy was the dominant theory, responsible for the creation of the Alliance. Realism also defined the purpose and course of action into the twenty-first century. This paper argues that realism

does not offer adequate solutions to combating climate change. As an alternative, this paper introduces Ulrich Beck's concept of the common risk society and Copenhagen School's theoretical framework, the constructivist school of international relations, as a theoretical framework through which climate change can be understood as a non-traditional security issue. Furthermore, the paper establishes the idea that climate change is a non-traditional threat that has multiplier effects on international security. The argument is strengthened by establishing a link between climate change impacts and negative consequences on socio-economic and political security. Lastly, the discussion shifts towards a review of NATO's policies, frameworks, and units responsible for addressing climate change as a non-traditional security threat.

This paper concludes that NATO has recognized the importance of climate change as a security threat, but that NATO's organizational mechanisms and divisions that are responsible for coping with climate change impacts are still evolving. This process faces new challenges, especially after the election of the U.S. President Donald Trump, who is highly skeptical regarding the issue of climate change. One must note, however, that in March 2017 U.S. Secretary of Defense James Mattis stated that climate change is already impacting operations of the U.S. armed forces and that combatant commands should incorporate these risks into their planning.^[3] Thus, it is clear that climate change is not completely excluded from the security agenda of the new administration in the White House. This paper emphasizes the broader idea that the climate change is a significant threat to security and that NATO should be one of the main players addressing this issue on the global level and serving as a role model for other states and regional organizations.

Traditional Views and the Realist Perception of Threat

The idea of security clearly distinguishes between military and non-military threats. Traditionally, the academic sphere of international relations has given more attention to so-called "hard" threats, which are roughly defined as military induced threats among and towards the states. This concept was established with the Westphalian peace treaty in 1648 and has remained a respected element of security doctrine into the twentieth and twenty-first centuries. A modern interpretation of this view on security was given by Walter Lippman in his book, *U.S. Foreign Policy: Shield of the Republic*. According to Lippman, "a nation is secure to the extent to which it is not in danger of having to sacrifice core values, if it wishes to avoid war, and is able to, if challenged, to maintain them by victory in such war."^[4] Lippman claims that the existence of the state revolves around security, which is divided into military and political security.

Realism is the oldest—and in military circles, the most respected—theory of international relations. The theory clearly provides answers to dilemmas such as why states go to war and how states should respond to potential threats. In general, realist scholars view security through four main assumptions, through which they define the international system. First, sovereign states are the main actors in the international system. States have governments, defined borders, and military might, all of which give them the legitimacy to rule and exercise power. Second, states live and act in an anarchic system. This philosophy came from seventeenth century English intellectual Thomas Hobbes, who coined the Latin phrase *bellum omnium contra omnes*, which translates into the 'war of all against all.' This dictum summarizes the idea that human nature, hence states, revolves around constant struggle and mistrust. Second, in an anarchic system, states are only interested in their own survival and perceive treats to be dangerous only when they rise to a level on which another state may be moved to exercise its military power. Third, realists believe that because the international system is driven by anarchy, all states seek to acquire power. This power offers security and survival. The drive to obtain power is the main force behind political interaction, arms races, and occasional security competition. Fourth, military power is the basic element that defines the strength of the state.

All realists agree on these four core assumptions. Nevertheless, various realist schools have different opinions about how states respond to threats. The views of *classical realist* views are best summarized in Hans Morgenthau's book, *Politics Among Nations*, in which the author implies that states are doomed to conflict because of humans' natural instinct for survival and our desire to acquire power.^[5] In Morgenthau's view, the only threat to states were other states. The essence of this thinking is focused on rational fears and natural inclinations, which in the classical realist point of view are natural human motives. While *structural realism* originated in classical realism, it differs from classical realism in the fact that it does not focus on human nature but rather on the actual structure of the international system. Structural realists, adherents to the views of

Kenneth Waltz, argue that the international system is anarchic and that in order to survive, states need to seek power.[6] While classical realists focus more on the anarchical character of human nature, structural realists emphasize their argument that the international political system is anarchic. Both schools, however, support the idea that threats to security are human- and/or state-inflicted.

Structural realism is further divided into *defensive realism* and *offensive realism*. Defensive realism is not concerned with the idea of maximization of state power. On the contrary, instead of maximizing power, states build enough capacity to allow them to survive by maintaining their position in the system.[7] Defensive realist Stephen Walt of Harvard University explains that states tend to form alliances in order to counter threats. When Walt refers to a threat, he is thinking of a scenario in which weaker states form an alliance to counter an attempt by a revisionist state to upset the balance of power.[8] Offensive realists support the same basic concept, but employ a different pattern of thinking. They claim that in order to survive, states need to amass as much power as they can. The most prominent offensive realist, John Mearsheimer, claims that interaction between states is dominated by a rational desire to achieve hegemony in a Hobbesian world.[9] Like classic and structural realists, their offensive and defensive colleagues perceive threat in the traditional state-centric form.

The youngest school of realism, *neorealism*, suggests that the behavior of states is not conditioned by motivations of power and security, but the internal structure of states. Randall Schweller, in his article “Unanswered Threats: A Neoclassical Realist Theory of Underbalancing,” describes how the internal capabilities of states will in the end determine the pattern of actions and success rates of their policies.[10] This theory offers a different realist-based explanation of how a state should react to external threats to its borders. Again, the main threat to state security is defined as traditional war.

Do realist thinkers view climate change as a threat to national security? Classical realists view climate change as an opportunity for states to seek power in competition with other states in order to secure their survival.[11] The problem starts with the idea that climate change is a threat that does not discriminate between borders and has multiplier effects across global ecosystems. This means that in order for states to survive and mitigate threats, they must work on multilateral environmental agreements and protocols, adopt domestic environmental legislation, and cooperate in international environmental organizations and institutions. Offensive realism sees climate change as an opportunity for one state to maximize its military capabilities while better preparing itself for potential climate challenges, while other states could use funds to recover from catastrophes caused by climate change.[12] This approach is very shortsighted and does not focus on finding solutions to deal with the threat. Defensive realism enhances the idea that immediate advantages like the formation of temporary alliances are more attractive to a state’s survival *modus operandi* than long-term considerations such as ratification of climate agreements.[13] Advocates of this school think that the international system of cooperation provides only short-term gains, which result in moderate change in the behavior of states.

Neoclassical realists claim that states with democratic institutional settings will continue to focus on the immediate advantages of fossil fuel energy while states with socialist governments will be better positioned to deal with climate change.[14] This is also a very narrow and non-flexible understanding. Consider, for instance, that the largest global carbon dioxide (CO₂) emitter in the world is communist China, while, for example, democratic Scandinavian countries are states with extremely environmentally friendly policies.

The biggest drawback of the realist pattern of thinking is the fact that it does not include threats originating from nature. Another problem of realism is its failure to recognize the trans-border and non-traditional threat multiplier character of climate change. Realists view cooperation between states as an action of last resort, but proper mitigation of climate change can only be achieved through extensive global cooperation and action.

Realism provides an effective insight into states’ behaviors and actions when it comes to traditional war, intra-state conflict, geopolitics, alliances, and the balance of power. Nonetheless, realist theory is quite limited when it comes to defining climate change as a threat and providing answers as to how states should act with respect to it. As the analysis of the different schools of realism showed, all of them have very little to offer when it comes to mitigating climate change. According to realists, states are driven by the wish to gain power on the expense of other states. When faced with environmental disasters caused by climate change, however, states actually need to cooperate in order to mitigate the negative impacts of climate change. Realist logic implies that

states should focus on maximizing their power rather than cooperating to protect the planet. Climate change does not fall into any of these categories. For that reason, the theory does not provide an adequate insight to climate change as a serious threat to global security.

Definition of Security beyond Realism and Climate Change as a Non-Traditional Threat

Richard Ullman redefined the notion of threat to states when he analyzed the concept of non-military threats arising from outside the state-centric perspective, writing

[A] threat to national security is an action or sequence of events that (1) threatens drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available to the government of a state or to private, nongovernmental entities (persons, groups, corporations) within the state.^[15]

In his essay, “National Security as an Ambiguous Symbol,” Arnold Wolfers argues that states vary considerably among themselves on how they rank security threats within their national agendas. Wolfers tries to explain that the international affairs arena is not a game where all states compete by the same rules in order to achieve same goals. “After all that has been said, little is left of the sweeping generalization that in actual practice nations, guided by their national security interests, tend to pursue uniform and therefore imitable policy of security.”^[16] For states, security—including threats—is an ambiguous symbol that they define alongside their needs at certain time periods and not according to a prescribed pattern of power maximization.

Climate change is definitely not a traditional threat to security. It is a planetary scale threat for people of different classes, different nations, different political ideologies, different countries, and it is hard to predict. The definition of climate change as a non-traditional threat to societies is well summarized in Ulrich Beck’s explanation of the risk society concept as a “systematic way of dealing with hazards and insecurities induced and introduced by modernization.”^[17] Beck tries to explain that states’ policies and perceptions are shaped by experiences from the past. In his view, these experiences encourage states to build their national defense system according to the risks that can be easily calculated and controlled. Nevertheless, the problem arises when countries’ security wellbeing is exposed to non-traditional threats that cannot be easily calculated. Beck writes, “Risk is ambivalence. Being at risk is the way of being and ruling in the world of modernity; being at global risk is the human condition at the beginning of the twenty-first century.”^[18]

Understanding climate change as a security threat means understanding security in the twenty-first century. In the traditional sense, security revolves around the idea of survival. Buzan, Waever, and de Wilde of the Copenhagen School introduced the theory that the existential threats to security depend on the “relation to the particular character of the referent object in question.”^[19] There is no universal standard that can define threats. The environmental sector encompasses broad fields of threats to security; it ranges from issues of survival of the species to large-scale issues such as minimizing the impact of big floods. Non-traditional threats are harder to define and require different response strategies because they focus on the relationship between human civilization and the biosphere, and not on the relationship among states themselves. Climate change impacts cause two types of threats: (i) easily securitized (e.g. survival of human civilization); and (ii) non-easily securitized (e.g. destruction of the entire ecosystem).

Unlike traditional security threats that imply the ignition of one security risk at different points of time, it is possible—perhaps even likely—that climate change may initiate multiple chronic conditions, which could occur simultaneously on a global level. In 2014, U.S. Secretary of Defense Chuck Hagel unveiled the Pentagon’s Climate Change Adaptation Roadmap. The central argument of this document is that climate change is a threat capable of multiplying and aggravating already existing problems (water shortages, droughts, etc.) as well as generating fertile ground for future security threats.^[20] Climate change is able to accelerate instability and exacerbate other drivers of insecurity that will simultaneously affect the environmental, economic, social, and political fabric of any modern society.

Nonetheless, the theory of climate security has been exposed to criticism. Alan Dupont, an academic at the University of Sydney, states that environmental threats are not going to act as main triggers of major conflict between states.^[21] In his opinion, climate change impacts complicate existing disputes and create tensions, but

they do not act as a direct cause of conflict. Daniel Deudney, a professor of Political Science at Johns Hopkins University with strong connections to the theory of geopolitics and republicanism, is completely against the idea of environmental security. According to Deudney, the concept of national security is centered on the idea of organized violence.[22] Hence, he argues that natural disasters are elements of unorganized violence that cannot be included under the umbrella of national security doctrine. In his view, national security planning is characterized by a zero-sum assessment, nationalism, and power maximization. Therefore, threats from climate change are not logical inputs to any of these concepts and including them in security calculations only creates confusion in the political leadership and makes them prone to conducting an impetuous foreign policy.

Deudney's concept of national security as organized violence is in complete contrast to the national security policies of some European Union (EU) and NATO member states. Addressing climate change through the mitigation principle has been firmly integrated into EU-wide 20-20-20 greenhouse gases (GHGs) policy reduction targets.[23] Correspondingly, in 2016 the German government issued a white paper, which categorizes climate change as permanent item on its national security agenda.[24] Beck classifies climate change as a threat that is so large it cannot be contained on the national level, but is more a concern with global implications. Moreover, he argues the following on the notion of global risk, "The experience of global risks is an occurrence of abrupt and fully conscious confrontation with the apparently excluded other. Global risks tear down national boundaries and jumble together the native with the foreign." [25]

Wolfers agrees that the nature and source of a threat define the scope of security. Securitizing climate change is necessary because climate change is inseparable from human security. At present, traditional security discourse must reexamine its state-centric conceptual approach to security. A monodisciplinary approach that emphasizes the maximization of power is highly unlikely to comprehend and respond to the serious existential challenges facing humanity in the twenty-first century. In order to properly confront the threat of climate change, states will need to develop an interdisciplinary approach that includes the inputs of a range of experts from environmentalists to defense specialists.

Climate Change as a Non-Traditional Threat Multiplier

Since its formation, the earth's climate has been changing. The planet has witnessed multiple periods of climate change that lasted for thousands of years, during which the earth's climate has been warming. The current global warming phenomenon is mostly caused by increasing concentrations of GHGs and other anthropogenic activities. Based on the measurements in ice core samples, scientists have come to the conclusion that present-day GHGs levels are the highest they have been since 800,000 years ago.

In the early nineteenth century, the concentration of CO₂ in the atmosphere was 280 parts per million by volume (ppmv). By the 1960s, emissions rose to 316 ppmv. Today they are around 420 ppmv.[26] The Intergovernmental Panel on Climate Change (IPCC) temperature threshold defined a "tolerable" increase in global average temperatures as an increase of only 2 degrees Celsius (°C). If the current emissions trajectories hold, however, humanity is heading towards a 5°C increase in average global temperature by the end of the twenty-first century.[27] Even though a 5°C increase sounds like an insignificant number, when observed on a planetary scale, it certainly represents a tremendous fluctuation. The temperature difference between today's temperature and the average global temperature during the last Ice Age was -5°C. During that period, significant parts of North America, Northern Europe, the Atlantic, and the Pacific oceans were covered with huge ice sheets.

Climate change is not principally an environmental concern, however. It is actually a problem that is closely linked to national economic policy, strategic planning, public health, infrastructure, finance, and international security.[28] The impacts of climate change are already dramatically affecting food security, weather patterns, trade relations, access to fresh water, and mass migration. Scientists have already provided mountains of convincing evidence that global warming is distressing the life-support systems on which human beings and other species depend.[29] More importantly, these impacts are occurring much more quickly than some security experts and scientists had predicted. Sea levels are rising, snow and ice cover are decreasing, and both rainfall patterns and growing seasons are changing.

The biggest problem is that these changes are happening in a very short geological time scale. The earth's climate has certainly changed over time, but in the past these alterations—barring extraordinary events like meteor impacts—developed slowly and lasted for thousands of years. This slow pace of climate change gave flora and fauna enough time to adapt and evolve. Scientists Ignacio Quintero and John J. Wiens discovered that species evolve at steady rates at around 1°C per million years.^[30] Researchers from the IPCC stated that temperatures are going to rise between 2°C and 4°C in the next hundred years.^[31] When calculated, the results lead us to the grim finding “that matching projected changes for 2100 would require rates of niche evolution that are 10,000 times faster than rates typically observed among species.”^[32]

A recent study by the Organization for Economic Co-operation and Development (OECD) shows that the most economically vulnerable regions are Africa and Asia. Based on data compiled since the 1990s, the OECD projects that gross domestic product (GDP) losses in 2060 will amount to 3.3 percent for the Middle-East and Northern Africa; 3.7 percent for South-and South-East Asia; and 3.8 percent for Sub-Saharan Africa.^[33] Furthermore, GDP surges in Latin America, -1.5 percent by 2060, and Eurasia, which includes Europe, China, and Russia, in 2.1 percent GDP loss by 2060. In total, societies across the globe are facing a global average 2 percent of GDP loss.^[34]

Climate change will negatively affect food production in tropical and temperate climates. Crops are adversely affected by drought and other extreme weather events. In the last hundred years the world significantly increased its food production and experienced dynamic growth in population. “Exposed and/or vulnerable regions will suffer from risks to all aspects of food security, including food access, utilization, and price stability, and could even experience full breakdowns of food systems.”^[35] In the summer of 2013, for instance, Russia was hit by an extremely destructive drought. A state of emergency was declared in twenty regions across the country. In the end, a ten percent drop in Russian production caused a forty percent increase in global wheat markets.^[36] Since the early 2000s, Syrian President Bashar al-Assad enforced an agricultural strategy with a goal of attaining self-sufficiency in national food production. During the effort to increase agricultural output, the country overused its water reserves. To make matters worse, Syria was home to one million Iraqi refugees, which contributed to additional social stress. From 2006 to 2010, large parts of the country were hit by consecutive droughts. When drought hit again in 2011, desperate farmers went to the cities and started protesting; when mixed with a complex ethnic composition and social structure in crisis, the drought certainly contributed to increasing tensions.^[37] It is hard to claim that drought sparked the Syrian Civil War; however we can state that socio-economic despair triggered by successive droughts between 2006-2011 accelerated social unrest in that nation.^[38]

Climate change will create public health issues through increases in heat-stress mortality, tropical vector-borne diseases, urban air pollution problems, and decreases in cold-related illnesses. “Areas where malaria is currently endemic could experience intensified transmission (on the order of fifty to eighty million additional annual cases, relative to an estimated global background total of five hundred million cases).”^[39] Natural disasters between 1990 and 1999 killed 600,000 people.^[40] Extreme and unpredicted fluctuations in temperatures cause heat stress (hyperthermia) or extreme cold (hypothermia) that often end in heart and respiratory failure. In the summer of 2003, high temperatures caused an estimated 70,000 more deaths as compared to the average death rate in previous years.^[41] Warmer temperatures increase levels of evaporation and disturb rainfall patterns. This increases the risk of diarrhea, a disease that on average takes around two million lives annually. Diarrhea also increases the spread of trachoma, an eye infection that can lead to blindness.^[42]

Environmental disasters are able to severely hurt modern economies. When hurricane Sandy ravaged the east coast of the U.S. and parts of the Caribbean, an estimated 1.8 million structures and homes were destroyed or damaged. Economic losses surpassed US\$ 65 billion. Tourism was the hardest hit industry, with 10,000 job cuts and losses of US\$ 1 billion.^[43] In the aftermath of hurricane Katrina, US\$ 40 billion in claims were filed and the city of New Orleans' population decreased by 18 percent when compared to pre-storm levels.^[44] In one of their reports that surveyed more than 1,500 leading global private companies, the Carbon Disclosure Project stated that climate change is the main threat to business security. The report also stated that more than one third

of companies experienced disruption in production from rainfall or drought which caused a 31 percent increase in production costs.[45]

Pre-existing poverty multiplies the chances of failure when a state or region is faced with a massive flood or long drought. The majority of low-income countries are situated in tropical zones closer to the equator. On average they are hotter, which has traditionally limited their agricultural outputs, and as temperatures increase, the amount of agricultural output decreases further. For example, negative climate impacts are predicted to generate a welfare loss equivalent to a quarter of total income in sub-Saharan Africa and certain parts of Asia.[46] In 2011, Thailand was hit by unusually destructive floods. In total, sixty-five out of country's seventy-seven provinces were affected. They lasted from July 2011 until January 2012, affecting the everyday lives of 13 million people. Total losses were US\$ 45 billion, which classifies this event as one of the top five natural disasters in recorded history.[47]

Climate change can be classified as a threat multiplier for countries suffering from political instability and ethnic tensions. Socio-economic differences in the northern part of Nigeria, particularly in the Sahel region, are stark. In the last decade, more than hundred villages have been abandoned due to desertification. Migration and unrelated population growth have added supplementary stress to already unstable relations between ethnic groups in the Muslim north and Christian south. In 2010, this led to land disputes and uprisings that were fueled by religious differences in which approximately a thousand people lost their lives.[48] Moreover, amplified desertification of the Nigerian Sahel left many people in despair, strengthening the influence of terrorist organizations, such as Boko Haram, an al-Qaeda affiliate. Boko Haram used the power vacuum and inefficiency of the central national government to position itself as an ambassador, representing the grievances of northern Nigerians. Boko Haram's actions infringed upon the Nigerian government's ability to provide security.

NATO and Climate Change

NATO first defined and recognized environmental challenges as potential threat to security in 1969. The first organizational mechanism focusing on environmental challenges was the Committee on the Challenges of Modern Society (CCMS). CCMS utilized knowledge gained through networks of national experts working on scientific publications examining defense-related environmental issues. Teams of experts funded by member states tackled problems affecting ecosystems and quality of life through three to five year pilot studies, shorter term projects, conferences, workshops, and roundtables.[49]

In 2006, CCMS merged with NATO's Science for Peace and Security (SPS) Program. SPS is a policy tool and platform for dialogue based on scientific research, innovation, and knowledge exchange. It provides funding, expert advice, and support to NATO-led operations and activities developed with partner states. NATO defines the environmental sphere within two concepts: security and protection. First, environmental security reflects responses to security challenges originating from the physical and natural environment. Second, environmental protection is defined as safeguarding physical and natural environment from the detrimental impact of military activities.

Since the formation of the CCMS, NATO has tried to respect environmental principles and policies under all authorized conditions. For that reason, the Alliance formed two different bodies, the Environmental Protection Working Group (EPWG) and the Specialist Team on Energy Efficiency and Environmental Protection (STEEEP). The EPWG drafts NATO policies that diminish possible harmful impacts of military activities on the environment. The STEEEP integrates environmental protection and energy efficiency regulations into technical requirements and specifications for military hardware, equipment, and machinery.

However, the notion of climate change as a security threat remains underdeveloped, especially when compared to traditional security risks such as traditional war, weapons of mass destruction, and terrorism. The non-traditional threat of climate change was first institutionalized in NATO's agenda in the 2010 Strategic Concept for the Defense and Security of the Members of NATO. Point fifteen in the Security Environment section mentions the climate change in the following context,

Key environmental and resource constraints, including health risks, climate change, water scarcity and increasing energy needs will further shape the future security environment in areas of concern to NATO and have the potential to significantly affect NATO planning and operations.^[50]

Former Secretary General de Hoop Scheffer highlighted climate change as a non-traditional threat in 2008. His successor, Secretary General Fogh Rasmussen, integrated climate concerns into NATO's functioning mechanism. In 2009, General Secretary Rasmussen stated, "NATO should begin a discussion on how we—NATO as an organization, and individual Allies as well—can do better to address the security aspects of climate change."^[51]

It is clear that climate change has been on the Alliance's priority list for years prior to the 2010 Strategic Concept, but until the beginning of this decade it was not integrated into the NATO's agenda. The Emerging Security Challenges Division (ESCD) was established the same year as the Strategic Concept. The ESCD was established to respond to a growing range of non-traditional risks and challenges, with climate change being one of them. The division's goal is to monitor and anticipate threats arising from non-traditional risks and catapult non-traditional security challenges to the center of NATO's radar.

In 2013, NATO adopted the Green Defense framework, which "seeks to increase the Organization's operational effectiveness through changes in the use of energy, while saving resources and enhancing environmental sustainability."^[52] The framework highlights NATO's readiness to explore the smart energy domain. Additionally, work within the framework gave birth to the Smart Energy Team (SET), a working group that advises NATO on its efforts to help lower fuel and electricity consumption and identify practical energy-efficient solutions to the Alliance's military forces. The SET should lead to cuts in CO₂ emissions by the world's biggest armed force.

In January 2014, Jens Stoltenberg became the United Nations Special Envoy on Climate Change. The 2014 Wales Summit Declaration stated that climate change and increasing energy needs will shape the global security arena in the future. The Wales Declaration underlined that climate change-induced security concerns such as environmental and resource constraints, including health risks and water scarcity, will result in crises that will directly affect NATO. The declaration reinforced the Alliance's stance on the issue that climate change represents a new and growing threat to all NATO member states.

Shortly after the Wales Declaration, the NATO Parliamentary Assembly adopted Resolution 427 on Climate Change and International Security.^[53] The document acknowledges that climate change-related risks are significant threat multipliers, recognizes the need to work on climate action with efforts to strengthen the resilience of states, and praises the formation of the Green Defense Framework and the SET. NATO showed readiness and willingness to invest in collective defense and to work to develop capabilities to respond to climate change challenges. During his visit to Croatia in July 2015, General Secretary Stoltenberg emphasized:

Environment, climate change is critical for promoting development and peace and stability. Development is important both for development and for security. And security is important to provide the foundations for development and for addressing climate change.^[54]

At the moment, NATO is undergoing an evolutionary process in integrating the threat of climate change into the organization's *modus operandi*. While the notion of climate change has been recognized, acknowledged, and analyzed, it has not yet been fully integrated into the Alliance's operations. To date, climate change has been a strategic security threat that has for the most part been more actively pursued on the national level.

Consider the fact that the melting of the ice in the far north is making the Arctic more and more accessible. As the Arctic ice continues to retreat, trade routes will remain open for longer periods of time, increasing annual traffic of ships carrying goods and resources in the North. At present, no one owns the Arctic, but Canada, Denmark, Norway, Russia, and the United States have all laid different claims to territories on the Arctic. In 2007, Russia sent a diving team to position its flag on the sea floor underneath the ice cap. NATO member state Norway is already adopting a Smart Defense Strategy that centers around a strong focus on the Arctic, both with regards to funding and resource allocation. In 2009, the Norwegian Defense Force made a decision "to relocate the

Army's Headquarters functions to the Arctic town of Bodø—1,700 kilometers north of Oslo—[bolstering] Norway's commitment to establishing an integrated High North defense system.”[\[55\]](#)

Canada is another NATO member state that cares greatly about the Arctic sovereignty issue. Canada deployed Canadian Ranger units to help the indigenous population of the Canadian Arctic to ensure that northern communities are equipped with all necessary goods so that they may reap the benefits of economic activities. Maintaining functional population centers in the Arctic helps Canada protect its national sovereignty in the far North.

The United Kingdom (UK) has incorporated climate change in its national defense planning, introducing climate change study programs in its military staff colleges. In 2009, the British Ministry of Defence published guidance entitled “Defence in Changing Climate,” a document that outlines principal objectives and identifies concrete targets for GHGs reduction in the sphere of the UK's military concerns.[\[56\]](#) The Ministry's climate change strategy became effective in March 2012. Soon after the adoption of the strategy, the Ministry created the position of Climate and Energy Security Envoy to act as a focal point for representing this institution in the climate change and security realm.[\[57\]](#)

Spain formed a Military Emergencies Unit to respond to climate disasters. By 2012, this military unit had responded to ninety climate change-ignited disasters, most of them on domestic territory.[\[58\]](#) Defense strategy documents in Denmark, the Czech Republic, Germany, Italy, the Netherlands, and Poland all mention climate security, but do not yet have concrete mechanisms, units, and departments that respond to these security threats. The French military developed several climate and security projects, but has admitted that its leadership is just starting to acknowledge more seriously the importance of climate change in the national security nexus. In 2011, close to 4.5 percent of the French defense budget was allocated to financing environment and future defense policy. The Dutch government has invested millions of Euros in strengthening coastal flood defense mechanisms, and Denmark has allocated 2.2 percent of its defense budget to improve the climate change disaster response capacity of the Home Guard Command.[\[59\]](#)

The issue of climate change encompasses a broad spectrum of human security, which may or may not include national security. So far, the U.S. has made the most progress in addressing this issue, as compared to the other twenty-eight NATO members.

Under the 2007 Global Climate Change Security Oversight Act, the United States initiated a far more systematic program of research on global climate change impacts on military requirements, operations, doctrine, organization, training, material, logistics, personnel, and facilities and on the actions needed to address such impacts.[\[60\]](#)

The 2008 U.S. National Defense Authorization Act directed the U.S. Department of Defense to evaluate the capability of armed forces to respond to natural disaster (e.g. floods, wildfires, droughts, etc.) and other missions the armed forces may be asked to conduct domestically or in foreign countries.[\[61\]](#)

The Pentagon's 2014 Climate Change Adaptation Roadmap is a concise document that outlines the effects of extreme weather events and rising temperatures on military training, operations, acquisitions, and infrastructure. The document is designed to become the basis for long-term planning for security risks that arise from the increase in global temperatures. This report is significant because it utilizes strong language implying that climate change is not only a future, but rather a present security threat multiplier. In response to this document, the U.S. Department of Defense has: (i) collected historic data and potential future vulnerabilities from coastal locations and developed regional sea-level rise scenarios for 704 coastal locations; (ii) evaluated military installations' vulnerability to global warming impacts and directed military planners to incorporate climate change considerations into certain installation planning efforts; and (iii) demanded that the hazardous impacts of climate change be included in installation master planning as well as natural resource exploitation planning.[\[62\]](#)

The U.S. armed forces have been actively engaged in studying climate change as a security threat since the end of the Cold War. The U.S. Naval War College was the first institution that pointed out the potential impact

of climate change on future policymaking. The U.S. intelligence community, as well, has been monitoring risks emerging from climate change within the MEDEA program—a collaborative initiative among climate scientists and U.S. intelligence agencies—and has been issuing intelligence reports based on analysis of climate change-related security impacts since 2008.^[63]

Although the national defense agendas of some member states are ahead of NATO in responding to climate change impacts, NATO has been engaged in helping Partnership for Peace Program countries to mitigate natural disasters caused by or exacerbated by global warming. In May 2014, a low-pressure cyclone in Bosnia and Herzegovina caused the biggest floods and landslides in recorded history, with flood damages costing close to US\$ 2.2 billion.^[64] Although fewer than a hundred people died, a significant percentage of critical infrastructure—such as schools, hospitals, roads, and railroads—were destroyed or heavily damaged. In addition, the disaster created 2,100 active landslides across the mountainous Bosnian terrain and dislocated many of the 9,000 marked minefields. Twenty-one NATO members provided humanitarian aid, helicopters, rescue teams, medicines, blankets, and tents across Bosnia and Herzegovina. Upon the request of the Bosnian government, NATO activated the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), which conducted operations in flooded Bosnian territory. Eighteen NATO member states sent boats, water pumps, power generators, humanitarian aid, and helicopters. Without the engagement of NATO's EADRCC and NATO troops on the ground, Bosnia and Herzegovina would have faced serious if not impossible obstacles in its recovery efforts.

Climate change has already become a dangerous reality in the five Central Asian republics. Environmental mismanagement and limited climate-related disaster adaptation, combined with a naturally arid climate that has been profoundly affected by the global rise in temperatures, transformed the region into one that is now increasingly vulnerable to the effects of temperature fluctuations and water shortages. Over the last fifteen years, the rise in temperature melted one-third of all the region's glaciers.^[65]

Melting glaciers disrupt regional water flows. The largest rivers in the region originate in the mountainous republics of Tajikistan and Kyrgyzstan; both republics are home to some of the Soviet era's largest dams. At the same time that these glaciers are retreating, fresh water levels are additionally impacted by hydroelectric dams. Turkmenistan, Uzbekistan, and Kazakhstan are feeling the consequences of reduced downstream river flows. Tajikistan and Kyrgyzstan are trying to fight their water shortages by retaining a larger amount of water in the dam reservoirs, but as shortages are becoming more severe, there is less water left for the agricultural economies of downstream countries. From 2004 to 2009, NATO worked to support integrated water resources management for a wetlands restoration project in the Aral Sea basin.^[66] Additionally, NATO was engaged in a project using a comprehensive multidisciplinary approach to assess the geo-environmental security of the Toktogul hydroelectric power station, which is the largest of its kind in Central Asia.

It is clear that threats emanating from global warming will exceed national and regional scopes. Climate change is a threat operating on a planetary scale, simultaneously activating multiple security challenges. Climate impacts will directly affect military facilities, personnel, and hardware. NATO cannot ignore the perils of climate change. Conversely, the Alliance will become more actively engaged in dealing with it. Since the publishing of the Strategic Concept in 2010 NATO started addressing this problem. Nevertheless, the Alliance can improve and catch up in institutionalizing the notion of climate change at the heart of organization by harmonizing its policy with the efforts already done by American, British, Canadian, Norwegian, or any other member state governments that could offer good solutions. In 2009, the former General Secretary Fogh Rasmussen laid out a robust list of objectives for NATO which are still relevant when applied to current context.

Future prospects for NATO's involvement in the realm of climate change security could be paralyzed by U.S. President Donald Trump. Since the beginning of his presidential campaign as well as his presidency, Donald Trump has demonstrated skepticism towards climate change phenomenon.^[67] Moreover, key members of Trump's administration are climate change deniers (i.e. head of U.S. Environmental Protection Agency Scott Pruitt), fossil fuel industry lobbyists (i.e. U.S. Secretary of Interior Ryan Zinke), and former fossil fuel industry executives (i.e. U.S. Secretary of State Rex Tillerson). The new American administration has already started abolishing domestic initiatives to protect the climate and environment and seems likely to ignore climate change security as a component of wider NATO policy and operations. It is still early to predict changes in the U.S.

official climate strategy within the Alliance; however, the U.S. withdrawal from the Paris Climate Agreement in June 2017 might have a negative impact on the Alliance's ability to integrate further climate change mitigation and adaptation measures as a security component of NATO's policy and operations.

Conclusion

Climate change is a non-traditional threat that has profound ramifications on a planetary scale. It simultaneously affects every person, rich and poor, as well as every state, big or small, developed or developing, young or old. Climate change is a threat multiplier that will shape the security environment in the twenty first century.

Although NATO is already engaged in developing policy and conducting operations responding to climate change impacts, it is easy to understand why climate change considerations are not yet fully integrated into the Alliance's *modus operandi*. After all, NATO was conceived in the Cold War and—at least until the September 11 attacks—its main purpose has always been to react to traditional threats. Climate change is just one of many threats to which NATO must respond. Realism offers good solutions to analyses of war, conflict, geopolitics, alliances, and balancing behaviors, but it lacks effective solutions when it comes to confronting environmental security threats originating from climate change.

Climate change is a novel non-traditional type of threat with multiplier effects that must be effectively addressed. Hence, as the discussion above demonstrated, the Alliance should address climate change through utilization of a non-traditional approach to security. Beck's risk society theory defines solid strategies to deal with climate change as a non-traditional threat multiplier. Risk society provides a theoretical framework for a systematic approach to dealing with hazards and insecurities induced and introduced by the process of modernization, of which climate change is a perfect example.

NATO will need to implement a stronger and more coherent approach to dealing with climate change. More precisely, the Alliance needs to develop more concrete policies as well as the capacities of partner nation forces to manage environmental security crises. This can include a faster process of sharing climate change-related knowledge between member states and the Alliance. This encompasses learning from capacities that exist on the member state level and upgrading them to work on the Alliance level. NATO militaries need to integrate issues related to climate risk into their training and exercise routines. Moreover, member states need to work on developing a common Alliance strategy for responding to the negative impacts of climate change on military planning and operations. Because there is currently a disparity about how this issue is addressed, all member states must be encouraged to integrate the mitigation of climate risks into their national defense strategies. The United States is currently led by a government that will most probably not focus on the issue, while its European allies such as France, Germany, and the UK already consider the mitigation of and adaptation to climate change to be one of their most crucial national security priorities. This difference in views has the potential to cause a certain level of disparity in strategic planning of the alliance. Nevertheless, the current U.S. administration's dismissal of this security concern could potentially complicate stronger engagement of the Alliance in the field of climate change security.

At present, NATO exists in a world where it is facing both traditional and non-traditional threats. It has proven itself as an organization that can master traditional threats, but the Alliance must upgrade and accelerate current efforts to develop a more efficient and concrete strategy to respond to the non-traditional threat multiplier of climate change as a security risk. This will require leaders to encourage efforts for deeper integration of climate change threat analysis into policy and planning within the Alliance's strategic thinking, because by doing so the Alliance will avoid paying higher security, economic, and social costs for the greatest problem that will confront humanity in the decades to come.

Acknowledgments

The author would like to thank the members of the editorial board of *Connections: The Quarterly Journal* as well as Maj. Patrick R. Heim for valuable comments and inputs during the writing stage and revision process of this research.

About the author

Amar Causevic is researcher at Global Economic Dynamics and the Biosphere program at the Royal Swedish Academy of Sciences. He was Partnership for Peace Program coordinator at the U.S. Department of Defense's Office of Defense Cooperation in Bosnia and Herzegovina. In addition, he worked on energy and climate change-related issues at the World Bank, Carbon War Room, and the USAID. Amar Causevic holds an MA in International Economics and Energy, Resources & Environment from Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS). *E-mail:* causevic.amar@gmail.com([link sends e-mail](#)).

-
- [1] Jürgen Scheffran, "Climate change and security," *Bulletin of the Atomic Scientists* 64, no. 2 (2008): 19-26, p. 22.
 - [2] Wendell C. King, "Climate Change: Implications for Defense," Intergovernmental Panel on Climate Change 5th Assessment Report, June 2014, available at http://gmacc.org/wp-content/uploads/2014/06/AR5_Summary_Defence.pdf([link is external](#)) (accessed April 2, 2016).
 - [3] Andrew Revkin, "Trump's defense chief cites climate change as national security challenge," *Science*, March 14, 2017, available at <http://www.sciencemag.org/news/2017/03/trump-s-defense-chief-cites-climate-change-national-security-challenge>([link is external](#)) (accessed April 18, 2017).
 - [4] Walter Lippman, *U.S. Foreign Policy: Shield of the Republic* (Boston: Little, Brown and Company, 1943), 53.
 - [5] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 5th ed., Revised (New York: Alfred A. Knopf, 1978), 4-15.
 - [6] Kenneth Waltz, *Theory of International Politics* (Long Grove: Waveland Press, 2010), 74-75.
 - [7] Waltz, *Theory of International Politics*, 179.
 - [8] Stephen M. Walt, "Alliance Formation and the Balance of World Power," *International Security* 9, no. 4 (Spring 1985): 3-43.
 - [9] John Mearsheimer, *The Tragedy of Great Power Politics* (New York City: W. W. Norton & Company, 2001), 4-7.
 - [10] Randall L. Schweller, "Unanswered Threats: A Neoclassical Realist Theory of Underbalancing," *International Security* 29, no. 2 (Fall 2004): 159-201, p. 160.
 - [11] John Baylis, Steve Smith, and Patricia Owens, *The Globalization of World Politics: An Introduction to International Relations*, 3rd ed. (Oxford: Oxford University Press, 2011), 99-100.
 - [12] Baylis, Smith, and Owens, *The Globalization of World Politics*, 105-106.
 - [13] Steve Smith, Amelia Hadfield, and Tim Dunne, *Foreign Policy: Theories, Actors, Cases*, 2nd ed. (Oxford: Oxford University Press, 2012), 193.
 - [14] Baylis, Smith, and Owens, *The Globalization of World Politics*, 106.
 - [15] Richard H. Ullman, "Redefining Security," *International Security* 8, no. 1 (Summer 1983): 129-153, p. 133.
 - [16] Arnold Wolfers, "'National Security' as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (December 1952): 481-502, quote on pp. 491-492.
 - [17] Ulrich Beck, *Risk Society, Towards a New Modernity* (London: Sage Publications, 1992), 260.
 - [18] Ulrich Beck, "Living in the World Risk Society," *Economy and Society* 35, no. 3 (August 2006): 329-345, p. 330.
 - [19] Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Publishers, 1998), 21.
 - [20] "2014 Climate Change Adaptation Roadmap," United States Department of Defense, October 13, 2014, available at <http://www.defense.gov/News/News-Releases/News-Release-View/Article/605221>([link is external](#)) (accessed March 10, 2016).
 - [21] Alan Dupont, "The Environment and Security in Pacific Asia," *ADELPHI Paper* 319 (June 1998), p. 76.

- [22] Daniel Deudney, "The Case Against Linking Environmental Degradation and National Security," *Journal of International Studies* 19, no. 3 (December 1990): 461-476, p. 461.
- [23] Branko Bosnjakovic, "Geopolitics of Climate Change: A Review," *Thermal Science* 16, no. 3 (2012): 629-654, p. 636.
- [24] "The 2016 White Paper on German Security Policy and the Future of the Bundeswehr," The Federal Government of Germany, July 13, 2016, available at <https://www.bmvg.de/resource/resource/./2016%20White%20Paper.pdf>(link is external) (accessed April 17, 2017).
- [25] Beck, "Living in the world risk society," p. 331.
- [26] Mark Maslin, *Climate Change: A Very Short Introduction* (Oxford: Oxford University Press, 2014), 29-45.
- [27] Fiona Harvey, "Everything You Need to Know about the Paris Climate Summit and UN Talks," *The Guardian*, June 2, 2015, available at www.theguardian.com/environment/2015/jun/02/everything-you-need-to-know-about-the-paris-climate-summit-and-un-talks(link is external) (accessed March 12, 2016).
- [28] Carol Dumaine and Irving Mintzer, "Confronting Climate Change and Reframing Security," *SAIS Review of International Affairs* 35, no. 1 (2015): 5-16, p. 6.
- [29] Janet Sawin, "Global Security Brief #3: Climate Change Poses Greater Security Threat than Terrorism," World Watch Institute, January 2016, available at <http://www.worldwatch.org/node/77>(link is external) (accessed February 25, 2016).
- [30] Ignacio Quintero and John J. Wiens, "Rates of Projected Climate Change Dramatically Exceed Past Rates of Climatic Niche Evolution among Vertebrate Species," *Ecology Letters* 16, no. 8 (2013): 1095-1103, p. 1095.
- [31] Quintero and Wiens, "Rates of Projected Climate Change Dramatically Exceed Past Rates."
- [32] Quintero and Wiens, "Rates of Projected Climate Change Dramatically Exceed Past Rates."
- [33] "The Economic Consequences of Climate Change," Organization for Economic Co-operation and Development, November 3, 2015, available at http://www.oecd-ilibrary.org/environment/the-economic-consequences-of-climate-change_9789264235410-en(link is external) (accessed April 5, 2016).
- [34] "The Economic Consequences of Climate Change."
- [35] Philippe Vitel, "Climate Change, International Security and the Way to Paris 2015," North Atlantic Treaty Organization Parliamentary Assembly, March 20, 2015, available at <http://www.nato-pa.int/Default.asp?SHORTCUT=3767>(link is external) (accessed January 20, 2016).
- [36] Javier Blas, "Wheat Soars after Russian Crop Failure," *Financial Times*, November 8, 2012, available at <http://www.ft.com/cms/s/0/7cbc024c-2998-11e2-a5ca-00144feabdc0.html>(link is external) (accessed March 25, 2016).
- [37] Caitlin E. Werrell, Francesco Femia, and Troy Sternber, "Did We See It Coming? State Fragility, Climate Vulnerability, and the Uprisings in Syria and Egypt," *SAIS Review of International Affairs* 35, no. 1 (2015): 29-46, p. 33.
- [38] Mark Fischetti, "Climate Change Hastened Syria's Civil War," *Scientific American*, March 2, 2015, available at <http://www.scientificamerican.com/article/climate-change-hastened-the-syrian-war/>(link is external) (accessed March 25, 2016).
- [39] "Climate Change and Health," Film (July 2011), World Health Organization video, 7:03, Posted July 19, 2011, available at www.youtube.com/watch?v=Z5gtjhWJ-3M(link is external) (accessed January 28, 2016).
- [40] "Ten Facts on Climate Change and Health," World Health Organization, October 2012, available at http://www.who.int/features/factfiles/climate_change/en/(link is external)(accessed January 28, 2016).
- [41] "Ten Facts on Climate Change and Health."
- [42] "Ten Facts on Climate Change and Health."
- [43] Diana Liverman and Amy Glasmeier, "What Are the Economic Consequences of Climate Change?" *The Atlantic*, April 22, 2014, available at www.theatlantic.com/business/archive/2014/04/the-economic-case-for-acting-on-climate-change/360995/(link is external) (accessed January 29, 2016).
- [44] Liverman and Glasmeier, "What Are the Economic Consequences of Climate Change?"
- [45] Beth Platow, "Climate Change and the Supply Chain," *Fronetics*, July 22, 2015, available at <http://www.fronetics.com/climate-change-and-the-supply-chain/>(link is external) (accessed March 3, 2016).
- [46] Richard Tol, "The Economic Effects of Climate," *Journal of Economic Perspectives* 23, no. 2 (2009): 29-51, p. 35.
- [47] "2011 Thailand Floods," *AON Benfield*, March 14, 2012, available at http://thoughtleadership.aonbenfield.com/Documents/20120314_impact_forecasting_thailand_flood_event_recap.pdf(link is external) (accessed April 7, 2016).
- [48] Marcus DuBois King and Jay Gulledege, "The Climate Change and Energy Security Nexus," *Fletcher Forum of World Affairs* 25, no. 44 (2013): 25-44, p. 30.
- [49] "The Committee on the Challenges of Modern Society," North Atlantic Treaty Organization, available at <http://www.nato.int/events/0110eapc/english/txt-15.htm>(link is external) (accessed January 21, 2016).

- [50] "Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization," North Atlantic Treaty Organization, November 20, 2010, available at <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>(link is external) (accessed January 16, 2016).
- [51] "Speech by NATO Secretary General Anders Fogh Rasmussen on Emerging Security Risks, Lloyd's of London," North Atlantic Treaty Organization, October 1, 2009, available at www.nato.int/cps/en/natolive/opinions_57785.htm(link is external) (accessed February 14, 2016).
- [52] "NATO Stresses Climate Change Impacts on Security," International Institute for Sustainable Development, September 2014, available at <http://climate-1.iisd.org/news/nato-stresses-climate-change-impacts-on-security/change>(link is external) (accessed February 12, 2016).
- [53] "Resolution 427 on Climate Change and International Security," North Atlantic Treaty Organization Parliamentary Assembly, October 2015, available at <https://www.actu-environnement.com/media/pdf/news-25462-resolution-otan-2015.pdf>(link is external) (accessed April 14, 2017).
- [54] Jens Stoltenberg, "NATO Secretary General Jens Stoltenberg at the Opening Session of the Croatia Forum," North Atlantic Treaty Organization, July 10, 2015, available at http://www.nato.int/cps/en/natohq/opinions_121655.htm(link is external) (accessed April 14, 2017).
- [55] Gerard O'Dwyer, "Norway Prioritizes High North Equipment," Defense News, March 11, 2015, available at <http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/03/norway-russia-arctic-northern-high-north-archer-cv90/2...>(link is external) (accessed April 10, 2016).
- [56] Michael Brzoska, "Climate change and the military in China, Russia, the United Kingdom, and the United States," *Bulletin of the Atomic Scientists* 62, no. 2 (2012): 43-54, p. 48.
- [57] United Kingdom Ministry of Defence, "Defence Infrastructure Organisation estate and sustainable development: How the Ministry of Defence estate is adapting to climate change, including nature conservation on the estate," June 21, 2013, available at <https://www.gov.uk/guidance/defence-infrastructure-organisation-estate-and-sustainable-development>(link is external) (accessed April 11, 2016).
- [58] Richard Youngs, *Climate Change and European Security* (New York: Routledge, 2014), 75.
- [59] Youngs, *Climate Change and European Security*, 81.
- [60] Richard Youngs, "Climate Change and EU Security Policy: An Unmet Challenge," Carnegie Endowment for International Peace, May 2014, available at http://carnegieendowment.org/files/climate_change_eu_security.pdf(link is external) (accessed April 12, 2016).
- [61] Michael Brzoska, "Climate change and the military in China, Russia, the United Kingdom, and the United States," 45.
- [62] "DoD Can Improve Infrastructure Planning and Processes to Better Account for Potential Impacts," United States Government Accountability Office, May 2014, available at <http://www.gao.gov/assets/670/663734.pdf>(link is external) (accessed April 4, 2016).
- [63] Caitlin Werrell and Francesco Femia, "Chronology of Military and Intelligence Concerns about Climate Change," The Center for Climate & Security, January 12, 2017, available at <https://climateandsecurity.org/2017/01/12/chronology-of-the-u-s-military-and-intelligence-communitys-concern-about-climate-change/>(link is external) (accessed April 18, 2017).
- [64] "Bosnia and Herzegovina Recovery Needs Assessment," European Commission, May 19, 2014, available at http://ec.europa.eu/enlargement/pdf/press_corner/floods/rna-executive-summary.pdf(link is external) (accessed April 12, 2016).
- [65] "The Glaciers of Central Asia: A Disappearing Resource," United Nations Development Program, December 2011, available at www.envsec.org/publications/brochure_the_glaciers_of_central_asia_dec_2011.pdf(link is external) (accessed April 10, 2016).
- [66] "NATO agrees to extend Environment and Security cooperation initiative," North Atlantic Treaty Organization, June 2010, available at www.nato.int/cps/en/natohq/news_64466.htm(link is external) (accessed April 14, 2017).
- [67] Dana H. Allin, "President Trump," *Survival* 58, no. 6 (2016): 237-248, p. 246.

Cultural Foundations of Transparent Governments

Judith Reid

Abstract:

Defense Institution Building focuses on change management at the Ministry of Defense level. In order to make sustainable change in any government, the solution has to work through and with the culture of that society. There are ways to reduce hierarchy and uncertainty in national strategy development, national defense organization, legal constructs, human resource management, financial management, and educational processes. Cultures change from within. If advisors understand the cultural foundations at work, they can better help countries chart paths toward sustainable, transparent governance.

Introduction

Governments are reflections of the people they serve. Each society has its own culture, its own set of subconscious rules that facilitate communication, determine acceptable behavior, and guide the community's interactions. In order to maximize success, the U.S. Department of Defense's (DoD) program to facilitate improved Defense Institution Building (DIB) in other states needs to work within the cultural foundations of the partner nations it engages in defense reform.

A common cultural profile in countries ruled by dictators includes very high power distance models and very high uncertainty avoidance. These are two of Geert Hofstede's cultural structures explained in *Culture's Consequences: International Differences in Work-Related Values*.^[1] This cultural model is found in many countries with authoritarian governments.

Hofstede created a way to compare the cultural structure of human groups. His first marker was a scale of hierarchy in society. If a society has rigid caste systems with numerous layers, then it has a high Power Distance Indicator (PDI). Movement between hierarchical layers is difficult, and there is almost total separation between the elite and those at the bottom of the pecking order. Centralized management, rigid inequality, and formal rules and approvals from non-ending chains of superiors are all hallmarks of high PDI. Subordinate and superior relationships are based on emotion. While this behavior is mandated from on top, what keeps it locked in place are the perceptions of the people at the lower end of the hierarchy that this is just the way things are. Their acceptance of their low status is what keeps the PDI in place and thriving, not the insistence on inequality from the top of the chain. Hierarchies can be tall and rigid or have only a few impermeable layers. According to *Culture's Consequences*, numerous closed societies have a high PDI quotient.^[2]

Uncertainty Avoidance (UAI) is observed when members of a society would do almost anything to keep the status quo. The risk of the unknown is too frightful to ponder in these populations. These groups love structure, have lots of specific laws and rules, trust experts and technical solutions, and disdain uncertainty. Top managers do not focus on strategy, but rather on operations. Education is highly structured learning with clear right and wrong answers. Life may be unfair or even brutal, but in high UAI countries, understanding the rules and expected behavior are worth more than any potential gain from rocking the boat. This is one of the key reasons that change is so difficult to institute in some of the countries that need it the most. Many nations with autocratic rulers have high UAI quotients, according to Hofstede.^[3]

There are two more pillars of Hofstede's original work that have a lesser role in creating despotic governments: Individualism (IND) and Masculinity (MASC) Indices. In the Individualism Index, societies are gauged on a scale of individualism versus collectivism. Is there a sense of "being in this together" as a group, or is it "every man for himself?" In collective societies, relationships are more important than tasks, opinions are predetermined by group membership, and one's private life is not as important as the group's needs. Bosses and employees are more familial, and harmony and consensus are the ultimate goals.^[4] A piece of this construct is the identification of the primary group. Does society concern itself mostly with its individuals or nuclear families

(high IND), or the extended family, clan, or township, as seen in more collective societies (low IND)? Many non-democratic nations register as collective societies (low IND) on Hofstede's model.[5]

According to Hofstede's model, highly masculine societies are more competitive than cooperative; have strong rules; recognition and advancement are important; failing is considered disastrous; and management is decisive and aggressive. A more feminine society would be collaborative, nurturing, and focused on quality of life. Management in more feminine societies is by intuition and consensus and conflict is resolved by compromise and negotiation.[6]

The combination of high power distance and high uncertainty avoidance creates the cultural conditions for dictatorships to thrive.[7] Super strong hierarchies enforced by intimidation are paired with populations that fear the unknown (even if the status quo is dreadful). This combination of high PDI and high UAI results in societies bound by rule books, an inability to make decisions except at the highest level of an organization, fear-based group-think, and strong compartmentalization of ideas, organizations and goods. These behaviors result in opaque business processes and cultures of secrecy, and they are ripe for graft. In this sort of environment, without a strong desire to change among the people and long-term intervention from others, the face may change, but the dictator will remain.

Defense Institution Building

The Defense Institution Building (DIB) program of the U.S. Department of Defense (DoD), much like the rest of Defense Reform (DR), works to create transparent, democratic governance and institutions that support the rule of law and provide services to citizens. The program focuses in part on defense strategy; national defense organization; legal institutions; human and financial resource management; and educational processes.[8]

By its very presence, DIB constitutes change management. As a program, it is never forced upon another country. Rather the type and level of consultation a country might receive is negotiated through the U.S. Embassy, U.S. Department of Defense, and the designated Combatant Command. Receiving Ministries of Defense request help with everything from creating an NCO Corps to facilitating strategy development. Because governance is a reflection of the society it serves, any lasting change in governing processes must reach down into the country's cultural foundation to survive.

From a cultural perspective, in order to unlock a frozen high PDI and high UAI environment, a society must begin moving from a state of fear toward openness.[9] To unlock this dictatorial paradigm, work with the host nation must increase its society's overall sense of trust. One place to begin would be to improve the rule of law so the public begins to feel a sense of fairness. Prosecute corruption, since it feeds uncertainty avoidance. Improve critical thinking in the population, not just rote memorization. Help students learn to question the theory, the teacher, the authority. All of these actions help reduce fear and flatten out overly strong hierarchies.

Below are six common functions of DIB and the cultural direction necessary to move a society from one that craves a dictator to one that can support transparent governance. These functions include defense strategy; national defense organization; legal institutions; human resource management; financial management; and education.

Strategy

One of the key tenets of open, liberal democracy is a national security strategy wrapped around concepts of economic growth, self-preservation, and world alliances. A national security strategy addresses issues of concern to a nation's self-preservation: real and perceived enemies, control of the external environment, and sovereignty.

Having a national security strategy (NSS) that is open and made public can invite criticism and scrutiny to the country's political leaders. Under normal circumstances, those are ideas that should direct the subordinate strategies that lead to action. A country's national military strategy (NMS) should derive from the national security strategy. The NMS focuses priorities for the country's military assets. If part of one country's NSS is to protect its people, then part of its NMS could be consequence management. That could lead to the military being prepared to respond to natural and man-made disasters. Since the military is often one of the most organized and

deployable entities in any federal government, disaster response is a common mission of many countries' military land forces.

In a dictatorial government, there is often no public NMS, much less an open NSS. The overarching direction of the security apparatus and military focus are kept close, remain opaque, and are designed to keep the power brokers in place. Only the inner circle of generals knows some of the NMS. The rank and file do as they are told in a classic strong hierarchical framework. This leads to an organizational culture of secrecy reinforced through blind hierarchical obedience (PDI), coupled with the desire to keep the difficult status quo over the more grave fear of the unknown (UAI).

National Defense Organization

In order to protect secrecy and encourage blind obedience, countries with strong dictatorial governments create a small inner circle of trust surrounded by heavy bureaucracies with layer upon layer of redundant functions. Organizations are stove-piped and insulated from one another. A strong inner and outer group orientation is encouraged, with the inner circle excluding the greater organization, which makes the general organization mistrust other departments. Uncertainty is avoided at all costs. The rank and file know that there will be no surprises and that even simple decisions will be forwarded to the leadership. This creates governmental ministries that cannot and will not communicate with each other and that fail to serve the public.

Legal Institutions

The rule of law is key to shifting control from a strong man to common citizens. Open, democratic governments are structured with checks and balances among the executive, legislative, and judicial functions so that no one function can wrest control from the others. This system is not perfect in any country, but the continuance to strive toward transparency and fairness empowers standards of conduct, codes of military justice, ethical guidelines, and even whistle-blowing. The more these guidons of fairness prevail, the more trust society can grant to its government.

Human Resources Management

Dictatorial governments create human resource processes that divide and conquer. They are the opposite of a merit system. People are promoted based on name or affiliation, not on their abilities or what assets they may bring to the job. Those in power are protected by filling in the ranks with like-minded underlings whose most important asset is loyalty to the power brokers. Often, those on top are highly competitive, while the masses see themselves as one collective whole. The HR domain is where UAI can be structurally increased, since promoting only those loyal to the power brokers protects the power imbalance.

Financial Management

If the national security strategy is opaque, then the financial system could be compared to an underground maze of tunnels with only one map. Aided by its obscure nature, the financial system is designed to benefit the elite. Power and money are kept centrally controlled; the organization is divided into the "in" and "out" groups; the leadership is highly competitive while the masses react collectively; and any hint of uncertainty wreaks havoc on everyone. In these societies, even those at the bottom of the ladder prefer brutal treatment to the uncertainty of going after any other option. Since the people on the bottom of the pyramid continue to recognize the higher stature of the power brokers and perpetuate these strong hierarchies, they recognize and accept that the financial system is rigged against them and that it offers no fairness in financial matters. Bribes large and small become the norm as underpaid bureaucrats are forced to supplement their income, while the power brokers are rewarded by financial trickery.

Education

Good education broadens the mind and creates new neural pathways that can connect in innovative ways with other established disciplines. Training is skill development – teaching or improving a concrete skill set. In dictatorial environments, there is little true education within the defense department. Beyond the individual and advanced technical training, there are few opportunities to engage adult learning institutions. Teaching institutions simply indoctrinate the students.

Recognizing there is a Problem

Loyalty is an outgrowth of strong hierarchy mixed with strong uncertainty avoidance. When a group requires loyalty of its members as part of a whole mix of values, such as the US Army values of loyalty, duty, respect, selfless service, honor, integrity, and personal courage, then it is balanced. When loyalty is by far the most important characteristic required of members of the group, then the extremely high level of uncertainty avoidance of the body is evidenced. Add a strong hierarchy, and the result is a closed fraternity, a gang, a dictatorship.

On the “love-fear continuum,”^[10] the insistence on loyalty above all else is an outgrowth of fear. This fear manifests in strong hierarchies that keep people in their places, along with a fear of the unknown. Strong control by the power brokers is perceived as the cure to this two-headed fear. The greater the fear within the leadership and the people, the stronger the hierarchy and desire for absolute control by all levels of the society.

Unlocking the Paradigm

How does this environment of fear shift in the other direction toward care, toward openness, toward collaboration? First, fear has to be neutralized. Rule of law is a key lever in reducing corruption, lightening gray economies, and easing dictatorial strangleholds. When communities on the bottom of the hierarchy see that there can be legal justice meted out to those who would rule with impunity, then the rigidity of the hierarchy begins to soften.

Second, care must be infused. People at the bottom of society already largely understand cooperation since they have learned to lean on each other to survive. The seed is there and can grow from the roots to the stem and to the leaves as long as trust can start to flourish in the cultural environment. If the outlaws of society can be brought to justice, then societal trust can take root and grow.

This may be accelerated by making amends. In post-Apartheid South Africa, the Truth and Reconciliation Councils were designed to bring evil out into the open, make amends for it, ask forgiveness, and promise a change in future behavior. It was public, a bit brutal, and necessary for the Mandela era to take root.^[11] Is South Africa today a paradise of peace and love? It is moving in that direction – a direction of self-determination, expanding cultural identity, and collaborative governance.

A key shift in culture usually requires some sort of crisis to break the mold of fear and derisiveness. Change agents can include war, terrorist attack, famine, or even a decision to transform if the pain becomes unbearable. Some foresighted leaders have paved the way from highly competitive environments toward collaborative ones. Mikhail Gorbachev and his *glasnost* movement led to the dissolution of the Soviet Union. President FW de Klerk of South Africa eradicated Apartheid and led South Africa toward inclusionary politics. Numerous dictatorships in Latin America converted from totalitarian regimes to fledgling democracies in the 1990s.

This does not mean that any of these countries are bastions of fairness and peace today, but they are moving away from fear/secretary/competitiveness toward care/openness/cooperation. As these societies move toward openness and collaboration, societal trust gets ever stronger, the rule of law becomes the expectation, and the ability of an autocrat to take root subsides.

DIB Strategy to Increase Transparency

Let us return to Hofstede’s model and see how it can inform the DIB process. In order to reduce the cultural dimension that fosters dictatorial rule, NSS and NMS need to shift from opaque to transparent. They should no longer exist just for a leader’s protection and control, but rather should focus on the country’s security and military needs as a whole. The NSS and NMS should move toward collective and collaborative policies, and be open to transparent governance based on collective values rather than based on fear of the unknown with its concomitant need for control. In more openly democratic governance, strategies can be developed beyond the year of execution, looking three, five, or even ten years ahead.

National Defense Organizations that Increase Transparency

In an open society, national defense organizations are different from those in a dictatorial government. In an open society, the organizational structure is transparent. There may still be tall hierarchies in place, but the need

for absolute control is missing. Leadership roles in the organization are based on merit, not on some crazy puzzle of loyalty and patronage. In a healthy government, decisions are decentralized, and redundant organizations are eliminated.

Legal Constructs that Increase Transparency

The execution of rule of law is key to building citizen trust, reducing UAI and PDI. In a healthy government, there are Inspectors General, ethics committees, and whistle-blower protections. There are police departments that protect the peace, courts that rule fairly, and prisons that are humane. There is a sense of fairness for the general population, not a skewed balance that favors only the leadership. In an open government, corruption and graft are prosecuted.

Human Resources Management that Increase Transparency

Personnel systems are reflections of an organization's strategies. Are they designed to keep the powerful on top? Are promotions based upon loyalty to the leader, or do they benefit the organization's mission? To move away from fear, HR systems need to be based on merit and the benefit each person can bring to the organization. In some rigid hierarchies, position is based upon affiliation not performance. This includes countries with established aristocracies, and it filters down into many high PDI societies. In a healthy organization, the rank and file feel confident that they can bring most HR issues to their leadership and the HR department without retribution. Promotions and discipline are based on merit.

Financial Management to Increase Transparency

Part of this overall sense of fairness is to pay government workers a living salary. When wages are insufficient to live, when bonuses are based on loyalty, or when the rank and file have to rely on "transaction fees" to survive, then fear pervades and strong men rule. When families believe they have enough income to take care of their needs, then a cooperative spirit can ease into the competitive environment.

A financial system based on openness and collaboration also includes funding for social services such as basic health care, hospitals, and care for the indigent. Financial systems of governments that want to help society also include funds for infrastructure like roads, waterways, and transportation systems. All of these things lead toward economic growth and prosperity.

Because the financial systems mirror and fund the governmental system, in an open system of governance, there are also checks and balances on the books. There are systems of fair auditing, oversight of leaders with contracting authority, and mechanisms in place to report fraud waste and abuse of power and funds. All of these programs reduce uncertainty and aid the cultural shift toward democratic governance.

Education to Increase Transparency

Many believe that "knowledge is power." In a dictatorial government, knowledge is closely guarded. Critical information is kept centralized, and critical thinking is kept underground. Education is given only to the most loyal, and limited training is given to the masses. In a society with high Uncertainty Avoidance, students long for clear answers. There is a clearly accepted right answer, and every other is considered wrong. In fact, this black/white viewpoint is a microcosm of the greater society, where the line between right and wrong is clearly delineated and enforced. In Post-Soviet satellite countries, education in many defense colleges consisted of a lecturer reading four hours of content to a large group of students. Some might call this indoctrination, not education. Open, accessible education that nurtures critical thinking is a key component of open societies.

Conclusion

A population ensconced in dictatorial leadership will accept its place on the bottom of the hierarchy, the lack of open strategies or organizational structures, and the abuse of patronage just to keep uncertainty at bay. This society will accept that loyalty is the only important value, that resources are shared based on fidelity, and that advancement is only for the "in" group.

If DIB Programs are to take hold, then UAI must be reduced through enforced rule of law, living wages, and merit promotions. When rigid laws relax to become administrative policies that guide, then PDI softens and

absolute control eases. Decreases in both UAI and PDI make up the key groundwork needed to reduce dictatorial chokeholds on societies.

In order to make a fundamental change in any government, the solution has to work through and with the culture of that society. Cultures change from within. If advisors understand the cultural foundations at work, they can better help countries chart paths toward sustainable, transparent governance.

Disclaimer

The opinions expressed in this article are those of the author and do not reflect the policy of the U.S., German, or any other government.

About the author

Judith Reid works for the U.S. Department of Defense in security cooperation. She led the Defense Institution Building Program at US European Command from 2011-2015. Her doctorate focused on the relationship between cultural understanding and military mission success. *E-mail:* DrJudithReid@gmail.com(link sends e-mail).

-
- [1] Geert Hofstede, *Culture's Consequences: International Differences in Work-Related Values* (Newbury Park, CA: Sage, 1980).
 - [2] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind, Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York: McGraw-Hill, 2010), 76.
 - [3] Hofstede, *Culture's Consequences*, 203-217.
 - [4] Hofstede, *Culture's Consequences*, 124-130.
 - [5] Hofstede, *Cultures and Organizations*, 89-134.
 - [6] Hofstede, *Cultures and Organizations*, 135-186.
 - [7] Hofstede, *Cultures and Organizations*, 412-416.
 - [8] Office of the Under Secretary of Defense for Policy, "DoD Directive 5205.82 Defense Institution Building (DIB)," January 27, 2016.
 - [9] Richard Barrett, *Love, Fear and the Destiny of Nations: The Impact of the Evolution of Human Consciousness on World Affairs*, vol. 1 (Bath, UK: Fulfilling Books, 2012), 217-227.
 - [10] Barrett, *Love, Fear, and the Destiny of Nations*, 113-133.
 - [11] Steve York, director, *Confronting the Truth*, filmed for the United States Institute for Peace in 2004.

Military Professionalization Programs in Kazakhstan and the United States: How to Implement and What Will We Gain?

Sebastian Engels

Abstract:

The U.S. should remain committed to Central Asian security cooperation, but must carefully evaluate each program for merit and value added to U.S. security goals in the region. Programs designed to increase Kazakhstan's military professionalization will have the most significant impact towards accomplishing these goals. U.S. security cooperation efforts to foster the development of a non-commissioned officer corps as part of Kazakhstan's military would serve as an excellent example of effective professionalization and a way to further our strategic relationships with non-NATO countries. Training programs that professionalize the Kazakh military can offer a cost-effective way for the United States to further a lasting partnership with Central Asia's most stable country.

Introduction

U.S. policy in Kazakhstan is one of the strongest examples of successful defense cooperation with a non-NATO country. In recent years, however, the country's importance to U.S. strategy has diminished because of the drawdown of the Global War on Terror in Afghanistan and cuts to the U.S. military budget since 2014. In light of other competing priorities across the globe, one could argue that security cooperation with Kazakhstan is an inefficient use of resources; however, Russia's aggression in Ukraine and the ever-present threat of Islamic extremism provide sufficient justification to stay engaged in Central Asia. Training programs that professionalize the Kazakh military can offer a cost-effective way for the United States to further a lasting partnership with Central Asia's most stable country. These efforts must be nested within higher-level strategies, thoughtfully planned in coordination with the host-nation, carefully executed by appropriate personnel, and continually scrutinized to evaluate their value to both U.S. goals for the country and to Kazakhstan's military.

Goals and Desired Outcomes of Security Cooperation

The goals of security cooperation, as defined by the Defense Security Cooperation Agency's "Green Book," include building defense and security relationships that promote U.S. goals in partner nations and providing "U.S. forces with peacetime and contingency access to host nations."^[1] This access need not be actual physical space in the form of a base or a joint training exercise. Access could also come from potential future cooperation or sharing of intelligence. To gain this access, Offices of Military Cooperation (OMC) use varying techniques. In like-minded, liberal democracies, security cooperation comes easily. Security cooperation officers (SCOs) facilitate foreign military sales (FMS) or direct commercial sales (DCS) of equipment or training contracts.

In countries like Kazakhstan that face many challenges to security cooperation, SCOs must use different techniques, often subtler than those used with western countries. In these countries, SCOs employ tools like foreign military financing (FMF), joint exchanges, and international military education and training (IMET) or expanded IMET (E-IMET) programs. Through these and similar programs, SCOs embed scholars and U.S. security experts in military institutions, develop western-styled military education programs, and increase the capabilities of a country's professional military education (PME) programs. They arrange for U.S. military experts to conduct training of our partners' military personnel or send representatives of a foreign army to be trained in the U.S. There, training participants observe first-hand the liberal, democratic values that are instilled in our military. In Kazakhstan, where the U.S. must compete for influence with regional powers and does not maintain continuous military presence, the U.S. relies on security cooperation to keep open essential lines of communication.

Other specific U.S. security interests in Kazakhstan include stability and a goal of the country providing a bulwark against Islamic extremism. Foreign fighters from Central Asia returning to their homelands after being expelled from Syria and Iraq could prove dangerous to not only the regions' governments, but also to U.S. interests.[2] Support to Kazakhstan as a credible security partner is in the interest of the United States, especially should future regional operations in Afghanistan or elsewhere necessitate a renewal and expansion of direct military cooperation with Kazakhstan.

Detractors' Arguments against Investment in Kazakhstan

Detractors of U.S. investment in the Kazakhstan military argue that we have already squandered millions in the country without adding to regional security or furthering our goals in the region. With ongoing conflicts in Iraq, Syria, and Afghanistan, along with increased focus on Russian aggression, increasing military aid to a currently peaceful and stable Kazakhstan seems to make little sense. Moreover, the U.S. National Security Strategy makes no reference to Kazakhstan at all and only mentions Central Asia once in reference to safeguarding their natural resources.[3]

Since the fall of the Soviet Union, Kazakhstan has spent relatively little on modernizing its armed forces, relying instead on the huge quantity of leftover Soviet equipment and systems.[4] Three separate defense doctrines took military spending in different directions. It was not until 2011 that Kazakhstan finally settled on a strategy for their military.[5] During this tumultuous time, the limited amount of U.S. aid designated for the country was largely wasted as a result of corruption and a poor defense system that was incapable of targeting programs with appropriate funding. Aside from the notable success of safeguarding materials formerly in Kazakhstan's weapons of mass destruction (WMD) complex, no significant defense reforms took place in Kazakhstan in the early years after the collapse of the Soviet Union.[6]

This changed after 9/11. As NATO and U.S. forces poured into Afghanistan, the U.S. needed to secure its supply lines. Kazakhstan agreed to allow NATO use of its airspace, part of the Northern Distribution Network (NDN), which was vital to U.S. logistics.[7] By 2010, a surge in Afghanistan by U.S. forces coincided with a surge of military aid to Central Asia, with a sizeable amount going to Kazakhstan. With increased aid, Kazakhstan instituted many of the promised military reforms and began work on an Individual Partnership Action Plan (IPAP) with NATO. By 2010, aid totaled \$649 million.[8]

By 2014, with a large drawdown in U.S. forces and lessening importance of the NDN, security aid dropped to \$148 million.[9] Additionally, as the U.S. pulled forces from the region, Russia and China began to slowly reassert their dominance. With a decreased need for Kazakhstan's airspace and the NDN, the strategic logistical importance of the country diminished. Today, Kazakhstan does not facilitate any U.S. military actions and Chinese and Russian proximity make it unlikely that we will soon have any sort of long-term deployment of troops in the country.

Critics of U.S. defense spending in Kazakhstan claim that the country is too closely tied militarily to Russia to ever be an effective partner with the U.S. Kazakhstan's military link with Russia remains intact and that will not change soon.[10] Russia also remains Kazakhstan's largest source of military equipment and training; over 500 cadets and officers from Kazakhstan train each year in Russian schools. Russia also maintains military establishments in Kazakhstan, including missile testing sites and the Baikonur *Cosmodrome*, the site of space launches.[11] Moreover, Kazakhstan is integral to Russia's air defense network and recently received new S-300 missile defense systems from Russia.[12] Kazakhstan's President Nursultan Nazarbayev was the only foreign leader at Russia's Victory Day parade in 2016 and, despite a cooling period after the Russian invasion of Ukraine, it is very unlikely that he can or will pull his country away from their closest ally. Kazakhstan will likely never join NATO, preferring to keep its IPAP, and will instead remain firmly within Russia's sphere of influence.

Why Professionalize Kazakhstan's Armed Forces?

Based on the political and military limitations outlined above and limited financial resources on the U.S. side, the U.S. should focus its security cooperation efforts in this country on what is both affordable and able to be achieved: professionalization of Kazakhstan's armed forces. Kazakhstan remains our closest partner in Central

Asia. We should strive to foster this partnership, but we cannot waste resources on ineffective or costly programs and—accepting the fact that China and Russia are the dominant powers in the region—concentrate on improving exploitable gaps in security cooperation, like military professionalization, to further our goals.

Military professionalization [\[13\]](#) accomplishes numerous shared goals more cheaply than other programs. First, Kazakhstan’s military will improve its capabilities and become better able to conduct its own independent actions domestically and abroad. Training with the U.S. will strengthen interoperability with NATO, increasing the chances of Kazakhstan participating in United Nations Peacekeeping operations with its Peace-Keeping Brigade (KAZBRIG), a long-term goal of Kazakhstan’s IPAP and, prior to 2014, the primary goal of the U.S. [\[14\]](#)

Second, civil society and good governance in Kazakhstan will improve. Liberal, democratic values will be introduced either directly in western-themed classes developed by the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes (PfPC), or through interactions with U.S. soldiers and civilians during exchanges or in U.S. military institutions. Evidence proves that countries that send military leaders to IMET programs in the U.S. are far more likely to advance their democratic reforms, a direct goal of IMET. [\[15\]](#)

Third, lasting and meaningful relationships will develop. From the ability to get to the heart of any matter with a trusted counterpart, to being able to make a personal request for support, these relationships advance U.S. interests. Kazakhstan yearns for diversification in its armed forces and independence from Russia. [\[16\]](#) Despite Kazakhstan’s current need of Russian support, the country aspires to improve aspects of its military that are beyond Russia’s capability, like developing a modern non-commissioned officer (NCO) corps, and improving their logistics, training management, and human resources (HR) systems. The U.S., boasting the most capable NCOs of any military, along with decades of our own professionalization efforts, could play a critical role in assisting to advance these goals.

Kazakhstan’s military professionalization efforts with the U.S. ensure that it will have an opportunity to expand its geopolitical environment by having bilateral access with the West. Cooperation also means a better U.S. understanding of the potential threats to Kazakhstan. By embedding ourselves in their institutions and academies, we will have a foundational understanding of their mindset on defense and be more able to influence their understanding of and perhaps even attitudes towards Western policy positions. [\[17\]](#) Attacks in Aktobe in June and Almaty in July 2016 by Kazakh citizens exemplify the internal threat most feared by the government. Having embedded experts in key positions may give the U.S. opportunities to influence Kazakh decision-making during times of crisis.

Finally, as tensions between Russia and the U.S. reach levels not seen since the Cold War, a capable mutual partner could serve as an intermediary in a rapprochement. Barring this, Kazakhstan could at least help facilitate cooperation in the event Russia and the U.S. find themselves pitted against a common challenge in the region, like Islamic extremism, and avoid the situation of limited cooperation currently seen in Syria. The U.S. would also gain an advocate at future negotiating tables with a country sharing cultural and historical ties with Russia.

U.S. Professionalization Strategy for Kazakhstan

The U.S. must carefully select approaches to assist in the professionalization of Kazakhstan’s armed forces, adhering to the following tenets:

1. Professionalization programs must nest with U.S. National Security, Combatant Command, and Embassy Country Team strategies.
2. All professionalization programs must derive from host-nation requests. The host-nation must invest in the program.
3. Partnerships need to develop with the right people and organizations.
4. The Office of Military Cooperation (OMC) must be the clearing house for all professionalization programs.

In a statement on Central Asia in 2014, General Lloyd J. Austin III, then Commander of U.S. Central Command (USCENTCOM) noted, “Going forward, initiatives will be tailored to transform our current limited transactional-based relationships into more constructive cooperative exchanges based on common interests and focused training.” [\[18\]](#) He later added that the U.S. has an important role in Central Asian security and that we

must empower these countries to combat their own regional threats. Specifically dealing with Kazakhstan, his strategy states:

The U.S.' relationship with Kazakhstan remains the most well-developed among the Central Asian states. The Kazakhs seek U.S. assistance in modernizing their military forces and we are taking advantage of the opportunity to further strengthen our bilateral relationship. Specifically, we are helping the Kazakhs to professionalize their non-commissioned officer corps, modernize their military education program, and improve training and personnel management.[19]

The current OMC in Astana's five year plan of cooperation with Kazakhstan envisions the formation of combat training programs, development of a training command for Kazakhstan, human resource development, logistics training, and other efforts to professionalize the armed forces.[20] Included in these efforts is the development of a PME program as well as specific calls to improve the NCO corps. As the plan makes clear, all efforts are to be based on requests from the host nation and focus on Kazakhstan's military as a whole, rather than on an individual unit or training center. The task of NCO development has the most established organization and the strongest support from both the embassy and Ministry of Defense (MoD) of Kazakhstan.[21]

NCO Development in Kazakhstan: Exemplifying Successful Military Professionalization

In 2003, Kazakhstan President Nursultan Nazarbayev deemed it necessary to professionalize Kazakhstan's military and introduce professional sergeants into the armed forces.[22] By 2010, NCOs were incorporated into military institutions, the National Defense University, and the Military Institute of Land Forces (ADI). Between 2013-2014, the Kazakh MoD created senior sergeant positions within its own headquarters and in its subordinate commands.[23] Commanders at the highest levels now have a senior enlisted advisor at their sides. An institution for decades within the U.S. military, these well-placed senior NCOs have immense power to influence decisions and increase the effectiveness of their forces. These steps to empower NCOs demonstrate Kazakhstan's own desire for NCO development.

Financial commitment by the U.S. to Kazakhstan began to decline in 2013, as the surge forces in Afghanistan started to withdraw and funding for Central Asia decreased, resulting in a shift in OMC priorities and moves away from overly ambitious objectives that had been goals of both Astana and Washington. These changes included a reduction in emphasis on the peacekeeping units, KAZBAT and KAZBRIG, that both states had once hoped would eventually participate in international operations, but which never deployed.[24] The team also decided to reduce efforts to equip Kazakhstan's military,[25] as equipping efforts in Central Asia did not always accomplish the stated goals and were at times plagued with problems.

The OMC drafted another five year plan in 2013, focusing on Kazakhstan's requests for NCO training. Unlike other, more controversial programs like Special Forces training or increasing Kazakhstan's intelligence network, NCO development did not trigger Russian objections about U.S. ambitions for the country. Kazakhstan was able to fully commit to the program without upsetting its careful balance between the two main regional powers, Russia and China. NCO development followed the second tenet of military professionalization, mentioned above, in that it derived directly from specific Kazakh requests that were backed by their own funding and supported by President Nazarbayev.[26]

Relationships as a Tool in Professionalization Efforts

The OMC concentrated on training NCOs and found a great partner to advance this effort – the current Command Sergeant Major of Kazakhstan's armed forces, Temyrbek Myrzakhanovich Khalykov. A two-time recipient of IMET funding and a U.S. Sergeants Major Academy international hall of fame student, Master Sergeant (MSG) Khalykov embodies a stated IMET goal, furthering “the understanding and defense cooperation between the United States and foreign countries.”[27]

In November 2014, MSG Khalykov first met with the Command Sergeant Major (CSM) of Army Central Command (ARCENT), CSM Ronnie Kelley, during a visit by the latter to Kazakhstan to discuss future NCO development endeavors.[28] CSM Kelley and MSG Khalykov met again in the U.S. at an ARCENT-funded exchange of NCOs in Fort Bliss, Texas. There, the two jointly planned a series of future professionalization

exchanges in the U.S. and Kazakhstan, leading to over fifteen events in fiscal year 2016, all advancing the cooperation between the NCO corps of the U.S. and Kazakhstan.[29] Between the end of 2014 and early 2016, CSM Kelley and MSG Khalykov collaborated face-to-face over ten times.

Kelley and Khalykov's relationship underlines the third tenet: partnerships need to develop with the right people and organizations. Rather than a one-time meeting, the two formed a lasting partnership.[30] In June 2015, CSM Kelley cancelled previous engagements and chose instead to attend Kazakhstan's first NCO Symposium. Though other nations' leaders were invited, Kelley was the only foreign dignitary at the event.[31] Prompted by this partnership, and those developed between the OMC and MoD, Kazakhstan requested more training.

One such request came after Kazakh leaders saw a U.S. Army basic training course at Fort Jackson, South Carolina.[32] Following that exchange, a team of U.S. NCOs from the USA Security Assistance Training and Management Organization (USA SATMO) started developing a curriculum for a drill sergeant course at Kazakhstan's NCO Academy.[33] The OMC prepared for the engagement, convening a meeting of the appropriate representatives before a Joint Senior NCO Consultation to allow SATMO NCOs and their Kazakh counterparts to plan and decide the program of instruction (POI).[34]

In April 2016, the SATMO team began a month-long training course at the Non-Commissioned Officer Academy (NCOA) in Shchuchinsk. This course focused on fundamental knowledge and skills taught to all incoming soldiers in the U.S. Army.[35] Initially, SATMO members instructed Kazakh NCOs on the POI, but after the Kazakh NCOs completed their own training plans, they instructed their peers. SATMO personnel mentored these NCOs and provided feedback on their courses, but Kazakh NCOs chose the materials and decided how the course should be executed.

Equally noteworthy was the support given by Kazakhstan's MoD. A public affairs team visited the training event and subsequently published several stories on the MoD's website, highlighting the partnership between SATMO and the NCOA.[36] The men from both countries worked, trained, ate, and slept under the same conditions for many weeks. Rather than a "cut-and-paste" POI handed to them by the U.S. NCOs, the Kazakh NCOs executed their own training plans, backed up with the support of the SATMO team.

The next phase of this operation includes plans to send Kazakh training teams to regional units, to focus on training NCOs at the small unit level. Alumni of the drill sergeant course will be in the lead for all training, with the SATMO team again in an advise and assist role. This train-the-trainer model, proven to work in the U.S. Army, creates subject matter experts among the land forces, improving the expertise of Kazakhstan's NCOs.

In August 2016, Kazakhstan held its second NCO Symposium, hosting ARCENT's new Senior Non-Commissioned Officer, CSM Eric C. Dostie, along with representatives of the U.S. Air Force Central and the Arizona Army and Air National Guard. Participants observed all the previous NCO development efforts and collaborated on future endeavors.[37] CSM Dostie, who coincidentally had attended the USA Sergeants Major Course with MSG Khalykov, remarked,

The significance of this being an NCO driven event is to show the relevance of the NCOs in today's armed forces ... It's amazing how they've [Kazakhstan] established an NCO corps and come so far in such a short time. The backing [by] the president and Minister of Defense shows how important this is to them.[38]

Command Sergeant Major Pavel Shishkin, the Ministry of Defense NCO Directorate Chief of Training and a 2009 graduate of the U.S. Sergeants Major Academy, also attended the event and underscored the success of NCO development:

During the past few years alone, we have completed more than 60 joint engagements with the U.S. forces and have shown to our commanders the necessity of the NCO corps. We have built trust by reassuring them that they can rely on our NCOs to achieve their goals ... The development of our NCO corps foundation was modeled after the U.S. with input and ideas from other nations. This process made it unique and original, tailored to fit our needs. We still are constantly improving our NCO corps and gaining insight from current models.[39]

Why U.S. Efforts toward NCO Development Work in Kazakhstan

All NCO professionalization efforts derived from the U.S. National Security, Combatant Command, and embassy country team strategies. General Austin put special emphasis on NCO development in his plan for the country; Kazakhstan's military professionalization still remains a focus. The OMC is likewise committed to the improvement of NCOs, with the full backing of the country team.[40]

Importantly, NCO development in Kazakhstan did not originate in a U.S. decision. As early as 1996, Kazakhstan began its own efforts to create a professional NCO corps. They funded and developed their own NCO Academy, graduating over 200 NCOs yearly, and revamped recruitment to attract skilled candidates.[41] They introduced NCOs into high staff positions and integrated them into their National Defense University. It is important to note that U.S. involvement in the programs originated in MoD requests in their five year cooperation plans. In other words, the Kazakhs requested and invested in the program. With this investment, the risk of them squandering support given by the U.S. was greatly reduced. Once involved, the U.S. side constantly communicated with the Kazakh leadership, MSGs Khalykov and Shishkin in particular, to ensure the accuracy of all programs.

The OMC screened all training, as the most knowledgeable on the needs of the host nation and the goals of the U.S. In some cases, the OMC facilitated a meeting by briefing U.S. personnel on key cultural sensitivities and garnering from the host nation their actual desires. Furthermore, the OMC judged the needs of a program and, because of the long-term relationships in play, received true feedback from participants on its effectiveness and relevance. If a program was deemed ineffective, the OMC either worked with the provider to adjust it or cancelled the activity.

As has been demonstrated by the relationship between CSM Kelley and MSG Khalykov and the partnership formed between USA SATMO and the NCOA, security cooperation is personality based. Leaders who partnered with foreign militaries needed cultural sensitivity, charisma, and sophisticated knowledge of their partner. Having foreign military experts, like the Foreign Area Officers in the OMC, available to guide and assist in the early stages of cooperation greatly contributed to the successful partnership.

Professionalization Problems

Other professionalization programs have not fared as well in Kazakhstan. Some of these programs followed some of the tenets outlined above, but neglected one or more and have ultimately failed. As mentioned above, human resources (HR) and logistics development are two examples. Both of these programs were requested by the MoD, but they have not succeeded.

Two anecdotes describe the situation. In 2015, a group of U.S. experts traveled to Kazakhstan with the goal of revamping their HR system. For a two-day period, totaling over fifteen hours, U.S. contractors lectured two Kazakh lieutenant colonels on HR reforms. One participant described the briefings as "pure torture." [42] The Kazakh officers were not decision makers, only representatives tasked to attend the briefings. In another series of U.S. lectures to MoD personnel, the intricacies of high-level logistics were spelled out in detail. Unfortunately, after the briefings, the Kazakh representatives revealed that they were actually interested in learning how the U.S. resupplies at the tactical level in Afghanistan.[43] As is the case with their HR system, Kazakh logistics are tied to Russia and large changes will not happen soon.

At some point, communication broke down between the participants of these programs; the proposed reforms were not formulated with sensitivity to this specific region. Unlike programs in the Baltics or Georgia, Kazakhstan was not asking for a complete overhaul of their systems. In HR and logistics, for instance, they want to institute minor reforms. They are interested, for instance, in U.S. recruitment practices and our Morale Welfare and Recreation (MWR) facilities. Likewise, in the area of logistics, they want to understand our tactical level resupply practices.[44]

Defense transformation is not an option. Their ties to Russia, fiscal constraints, and political realities make it impossible. There are no impending external threats, nor any crises calling for a new system of government. Unlike the Baltic States, who are NATO members, or Georgia, which desperately seeks membership, Kazakhstan only maintains an IPAP with NATO and will likely never seek full membership. This reduces the motivation to

change.[45] Even HR and logistics development programs have largely stalled. These endeavors in Kazakhstan can work, but the goals of each should originate from specific requests by the MoD, followed by joint planning to determine the POI, much like what was accomplished by USA SATMO and others.[46] Programs that are too broad or beyond the political capacity for change will falter.

The OMC must be the clearing house for all of these programs. In a recent panel discussion with former and current Office of Defense Cooperation and OMC Chiefs, concerns were raised about U.S. providers working within their countries, at times devoid of OMC oversight.[47] The chiefs derided these “summer employment programs,” claiming they can be a nuisance and, at worst, detrimental to security cooperation. Interestingly, the problem is pervasive enough that the chiefs each had different methods to mollify these individuals including creating scheduling conflicts, or more decisively, gaining the support of the ambassador to cancel a program.

Working at odds with U.S. personnel, who undoubtedly have good intentions, should not be a first resort to solve these issues. However, to be effective stewards of U.S. taxpayers’ dollars, the OMC must determine whether a provider’s program adheres to all four tenets, provides sufficient benefit to the U.S., and improves the capabilities of the host nation.

Conclusion

A well-designed and efficiently executed military professionalization programs is the instrument that is most likely to make a significant impact on the successful accomplishment of improved Kazakh military capabilities and the achievement of U.S. goals in Kazakhstan and the region. As demonstrated by the OMC’s advances in NCO development, appropriate techniques and procedures need to be followed. The right people and organizations from both sides need to cooperate, work together to build a fruitful relationship, and continually and jointly assess their endeavors. These efforts should originate in the expressed needs of our partner country and stem from the greater U.S. strategies, with the acknowledgement that the U.S. must carefully target its security cooperation. A true economy of force mission, security cooperation with Kazakhstan should be fiscally responsible and specifically tailored to achievable goals. If all tenets of professionalizing a force are followed, the U.S. is apt to gain much; we will influence the Kazakh military at a foundational level towards adopting western ideals while frugally enhancing a strategic partnership in Central Asia. Finally, those who serve in the professionalized armed forces of Kazakhstan, along with U.S.-trained leaders in key positions, will inspire their nation to continue its democratic advancement.

About the author

Captain **Sebastian Engels** is a U.S. Army Foreign Area Officer with a Eurasia regional focus. He studied Russian at the Defense Language Institute in Monterey, CA and then spent a year conducting In-Region Training, working in U.S. embassies and multi-national organizations, in former Soviet states. Presently, he is a M.A. Candidate at Harvard’s Davis Center in its Russia, Eastern Europe, Central Asia (REECA) program.

[1] Ernest B. McCallister, ed., *The Management of Security Cooperation: Green Book*, Edition 37.1 (Wright-Patterson Air Force Base, OH: The Defense Security Cooperation Agency, 2017), 1-1.

[2] Gregory Gleason and Roger Kangas, “Foreign Fighters and Regional Security in Central Asia,” *Security Insights* 17 (2017): 1-3.

[3] The United States National Security Strategy, *The White House*, February 2015, [https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf\(link is external\)](https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf(link%20is%20external)), 1.

- [4] Eugene Rumer, Richard Sokolsky, and Paul Stronski, "US Policy Toward Central Asia 3.0," *Carnegie Endowment for International Peace* (25 January 2016): 2, [http://carnegieendowment.org/2016/01/25/u.s.-policy-toward-central-asia-3.0-pub-62556\(link is external\)](http://carnegieendowment.org/2016/01/25/u.s.-policy-toward-central-asia-3.0-pub-62556(link%20is%20external)), accessed July 30, 2017.
- [5] Roger McDermott, *Kazakhstan's Defense Policy: An Assessment of the Trends* (Carlisle, PA: U.S. Army War College Press, 2009), 3.
- [6] Timur Shaymergenov and Marat Biekenov, "Kazakhstan and NATO: Evaluation of Cooperation Prospects," *Central Asia and the Caucasus* 11, no. 1 (2010): 35-41, quote on p. 39.
- [7] Rumer, Sokolsky, and Stronski, "US Policy Toward Central Asia 3.0," 7.
- [8] Rumer, Sokolsky, and Stronski, "US Policy Toward Central Asia 3.0," 7.
- [9] Rumer, Sokolsky, and Stronski, "US Policy Toward Central Asia 3.0," 7.
- [10] Mariya Y. Omelicheva, "Russia's 'Checks and Balances' on Kazakhstan's Quest for Military Independence," *Russian Analytical Digest* 188 (2016): 5-8.
- [11] Omelicheva, "Russia's 'Checks and Balances' on Kazakhstan's Quest," 6.
- [12] Catherine Putz, "Kazakhstan Takes Delivery of Free Russian S-300 Missile Defense Systems," *The Diplomat*, 9 June 2016, [http://thediplomat.com/2016/06/kazakhstan-takes-delivery-of-free-russian-s-300-missile-defense-systems\(link is external\)](http://thediplomat.com/2016/06/kazakhstan-takes-delivery-of-free-russian-s-300-missile-defense-systems(link%20is%20external)), accessed July 30, 2017.
- [13] Samuel Huntington and Marybeth Ulrich, experts on civil-military relations, include career development models; emphasis on training and professional military education; compatibility of military and societal values; and support and infrastructure for soldiers and families in their definitions of military professionalization. See Samuel P. Huntington, *The Soldier and State: The Theory and Politics of Civil-Military Relations* (Cambridge, MA: Belknap Press of Harvard University Press, 1957) and Marybeth Peterson Ulrich, *Democratizing Communist Militaries: The Cases of the Czech and Russian Armed Forces* (Ann Arbor, MI: The University of Michigan Press, 1999), 24-25.
- [14] Dmitry Gorenburg, "External Support for Central Asian Military and Security Forces," Working Paper (Stockholm: Stockholm International Peace Research Institute and Open Society Foundations, 2014), 59-61.
- [15] Carol Atkinson, "The Role of US Elite Military Schools in Promoting Intercultural Understanding and Democratic Governance," *All Azimuth* 4, no. 2 (2015): 19-29, quote on p. 27.
- [16] Omelicheva, "Russia's 'Checks and Balances' on Kazakhstan's Quest for Military Independence," 7.
- [17] Atkinson, "The Role of US Elite Military Schools," pp. 20-27.
- [18] U.S. House of Representatives, Committee on Armed Services, Hearing on Fiscal Year 2015 National Defense Authorization Budget Requests from the U.S. Pacific Command, U.S. Central Command, and U.S. Africa Command, Statement of General Lloyd J. Austin, CDR U.S. CENTCOM, on the Posture of U.S. CENTCOM, March 5, 2014.
- [19] Lloyd J. Austin III, "Statement of General Lloyd J. Austin III on the posture of U.S. Central Command," *US Central Command*: 2016, [http://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/\(link is external\)](http://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/(link%20is%20external)).
- [20] Author's interviews of personnel working in the U.S. Office of Military Cooperation in Kazakhstan, Astana, June-September 2016.
- [21] Author's interviews with OMC personnel.
- [22] McDermott, *Kazakhstan's Defense Policy*, 6.
- [23] The Office of Military Cooperation in Astana, "OMC NCO Initiatives," August 2016, Astana, Kazakhstan.
- [24] KAZBAT (battalion) and KAZBRIG (Brigade) never wholly deployed. A small contingent of Kazakh peacekeepers deployed to Iraq in 2003, but not as a unit and not independently.
- [25] Author's interviews with OMC personnel.
- [26] President Nazarbayev visited the NCO Academy in Shchuchinsk on several occasions in full military uniform and often publicly praises the Academy; author's interview, MoD senior leader, Shchuchinsk, Kazakhstan, July 2016.
- [27] U.S. Department of Defense and U.S. Department of State, "Foreign Military Training, Fiscal Years 2012 and 2013," II-1, II-2.
- [28] Author's interviews with OMC personnel.
- [29] Author's interviews with OMC personnel.
- [30] Assel Satubaldina, "Kazakhstan and US Need to Strengthen Military Cooperation: US Army Central Command Sergeant Major," *Tengrinews*, 17 June 2015, [http://en.tengrinews.kz/military/Kazakhstan-and-US-need-to-strengthen-military-cooperation-US-260820\(link is external\)](http://en.tengrinews.kz/military/Kazakhstan-and-US-need-to-strengthen-military-cooperation-US-260820(link%20is%20external)), accessed July 30, 2017.
- [31] Office of Military Cooperation in Astana, "After Action Review – Kazakhstan NCO Symposium," 2 July 2015, Astana.
- [32] Master Sgt. Gary Qualls, "Kazakhstan Army Visits US Army Central," *US Army*: 6 January 2016, [www.army.mil/article/160580/Kazakhstan_army_visits_US_Army_Central\(link is external\)](http://www.army.mil/article/160580/Kazakhstan_army_visits_US_Army_Central(link%20is%20external)), accessed July 30, 2017.
- [33] Author's interviews, USA Security Assistance Training and Management Organization members, July 2016, Shchuchinsk, Kazakhstan.

- [34] Office of Military Cooperation in Astana, “After Action Review, Joint Senior NCO Consultation,” National Defense University, Astana, 26-29 January 2015.
- [35] Ministry of Defense of Kazakhstan, “US specialists conduct advanced training of Drill Sergeants from the Armed Forces of the Republic of Kazakhstan,” 13 July 2016, <http://mod.gov.kz/rus/press-centr/novosti/?cid=0&rid=3022>(link is external), accessed July 30, 2017.
- [36] Ministry of Defense of Kazakhstan.
- [37] Author’s interviews with OMC Personnel.
- [38] SGT Aaron Ellerman, “Building Partnerships Abroad,” US Army, 2 September 2016, <https://www.army.mil/article/174536>(link is external), accessed July 30, 2017.
- [39] Ellerman, “Building Partnerships Abroad.”
- [40] The U.S. Ambassador has stated repeatedly that NCO Development is one of the most successful programs of security cooperation with Kazakhstan.
- [41] Author’s interviews with OMC personnel: Kazakhstan still minimally relies on conscription, but has repeatedly pledged to end the practice.
- [42] Author’s interviews with U.S. Embassy personnel, Astana, July-September 2016.
- [43] Author’s interviews with U.S. Embassy personnel.
- [44] Author’s interviews with U.S. Embassy personnel.
- [45] Shaymergenov and Biekenov, “Kazakhstan and NATO,” 39.
- [46] Another great example of successful partnership and adherence to the tenets outlined earlier in the text came from Partnership for Peace Consortium of Defense Academies and Security Studies Institutes (PfPC). Through a Defense Education Enhancement Program (DEEP) partnership, PfPC uses NATO’s NCO Reference Curriculum to develop the faculty and material in Kazakhstan’s NCO Academy.
- [47] Chiefs of Offices of Defense and Military Cooperation, “OMC and ODC Panel Discussion,” The George C. Marshall Center, Garmisch, Germany, September 2016.