AD SECURITATEM

The best essays by students at the Baltic Defence College during 2017/18

Contents

Foreword

Welcome to the fourth edition of *Ad Securitatem* featuring the best work written by the Joint Command and General Staff Course (JCGSC), Civil Servants Course (CSC) and the Higher Command Study Course (HCSC) students at the Baltic Defence College during the 2017/18 academic year.

The selected essays represent the aptitude of students of the 2017/18 JCGSC, 2017 CSC and 2018 HCSC. In their impressive work, the students share their professional knowledge, experience and ideas in an analytic and critical manner that hopefully provides food for thought to all readers.

Triinu Soomere

Lecturer, Critical Thinking and Communication

BEST ESSAYS OF THE JOINT COMMAND AND GENERAL STAFF COURSE (JCGSC)

Is the Operational Planning Process Immune to the Pitfalls of Group Decision-Making? MAJ Jeff Allen

Madness is the exception in individuals, but the rule in groups.
-Frederich Nietzsche

Introduction

Consider an efficient military headquarters, able to take every operation the commander conceptualizes, construct courses of action based on that vision, produce orders, and supervise subordinate units in its execution "to the letter." A loyal chief of staff keeps the "good idea guy" silent and everyone stays focused on fighting the plan. However, success does not come in operations as often as it should for this HQ. The chief planner, a graduate of the best staff college the western military world has to offer, is baffled*. We never experience the dissent seen in other HQs. Why are we getting it wrong? What are we missing?*

This fictitious headquarters may be suffering the effects of groupthink. While the operational planning process (OPP) practiced by the Canadian Armed Forces (CAF) and its NATO allies is a proven planning method for digesting complex military problems, this process is not immune to groupthink and other symptoms of flawed group decision-making. Education highlighting the common group decision-making errors and their causes is infrequent during officer training, although the USA, Canada and other allies are taking positive steps in this regard (Mulrine, 2008). This paper aims to compare parts of the OPP with current knowledge of group decision-making phenomena to show where the process remains vulnerable. Throughout, the CAF model of OPP as described in Joint Publication 5.0, *The Canadian Forces Operational Planning Process (2008)* will be used. In CAF doctrine, OPP is divided into five stages, with the following key outputs (Canadian Armed Forces, 2008) (Canadian Army Command and Staff College, 2010):

Stage	**Key Outputs**
1 – Initiation	- Preliminary Warning Order - Intelligence preparation initiated - Commander’s initial planning guidance issued
2 - Orientation	- Mission Analysis Briefing - Commander’s Planning Guidance - Warning Order
3 – Course of Action (COA) Development	- Information Briefing - COA comparison/wargame products - Decision Briefing - Concept of Operations (CONOPS)
4 – Plan Development	- Plans and orders
5 – Plan Review	- Fragmentary Orders - Branch/sequel planning

While most officers have a working knowledge of the OPP, an instructor of the US Army’s University of Foreign Military and Cultural Studies, commonly known as “Red Team University,” counsels that one cannot assume the same level of familiarity among military leaders with the groupthink phenomenon (Vore, 2013). Thus, this paper begins with a brief explanation of groupthink, and how it manifests itself in a military planning environment.

Next, to focus the analysis, we will investigate how flawed group decision-making may pervade specific activities in the OPP: the commander’s initial planning guidance; intelligence preparation of the battlefield (IPB); mission analysis; course of action (COA) development, and; plan development and execution. The effect of group dynamics on risk assessment also warrants consideration, since this process is firmly embedded in operational planning. Current efforts to mitigate group decision-making hazards in Canadian doctrine will be highlighted where they exist, but the final recommendations are a synthesis of several sources, including the author’s own experience.

Background - Groupthink

The term “groupthink” was coined by US psychologist Irving Janis in his 1972 publication, *Groupthink: A Psychological Study of Foreign Policy Decisions and Fiascoes,* and describes a condition of flawed group dynamics and decision-making. Janis distilled this phenomenon into eight indicators, adapted to the military context here:

- An illusion of invulnerability among the staff;
- A belief in the inherent morality of the operation;
- “Rationalizing away” information that may change the plan;
- Stereotyping (“templating”) the enemy;
- “Self-censorship” of group members in the interest of the collective;
- Illusions of unanimity (or lack of dissent);
- Suppression of dissenters; and
- The emergence of “mindguards.” (Janis, 1972)

Individually, these indicators may not cause flawed decision-making, but their existence, Janis theorized, lead to destructive behaviours such as self-censorship, discounting alternate viewpoints, or underestimating an adversary.

Groupthink is not a new challenge to military thinking, and the planning of Operation MARKET GARDEN through the Netherlands in September 1944 is an excellent example (Houghton, 2015). This operation, driven by the strong personality of Field Marshal Bernard Law Montgomery, was hastily ushered through the planning process in order to exploit a disorganized, withdrawing enemy and, hopefully, end World War II by Christmas 1944. As a result, its chief proponents displayed illusions of invulnerability against an underestimated enemy. Any dissenters, such as the UK 1st Airborne Corps intelligence officer Major Brian Urquhart (who furnished aerial reconnaissance photos suggesting the presence of a German panzer division) were summarily blockaded or dismissed (Ryan, 1974). In this case, the mindguards of the staff were opposed to scrapping the plan based on this critical intelligence; it had simply progressed too far. Also, the cohesive, close personal relationship between the senior leaders surrounding Montgomery in 1944 helped ensure unanimity, even if it was illusory. Ultimately, the effect of dropping the 1st UK Airborne Division over two German panzer divisions was disastrous.

While the term *groupthink* has a permanent place in organizational culture studies, Janis' theory is not without detractors from a social-scientific standpoint. In their 2015 publication, *Wiser*, Sunstein and Hastie warn, "Experimental research fails consistently to link particular group characteristics, including those that Janis emphasized, to groupthink" (Sunstein, et al., 2015). However, we can acknowledge that, while considered merely an empirical work of literature by some social scientists, the groupthink theory and the research it spawned has given leaders valuable insight into the hazards of group decision-making.

Commander's Initial Planning Guidance

OPP is a command-driven process (Canadian Armed Forces, 2007), and one of the earliest points of influence for a commander upon receipt of a mission is through the commander's initial planning guidance. Whether formally or informally delivered, a commander may include a personal assessment of the situation (ahead of IPB), state initial information requirements, and direct modifications (often due to lack of time) to the planning cycle right at the outset of OPP (Canadian Army Command and Staff College, 2010). The first two actions risk introducing bias among the staff by prematurely focusing planning effort and rejecting innovative options – an example of the phenomenon that "the decision is often made based on who spoke first" (Sunstein, et al., 2015). An over-prescriptive initial planning guidance, while in the interests of speedy plan development (Canadian Armed Forces, 2007), contradicts some of the best practices in fostering creativity developed by the business community, and in fact may hamper the staff's creativity in the COA development stage. Here, the observations of Sunstein and Hastie in their book, *Wiser*, are explicit:

> "There's a lesson for foolish groups whose leaders often announce a preference for a proposed course of action before the groups have gathered adequate information or aired possible outcomes: […] if a project, business, politician, or cause gets a lot of early support, it can turn out to be the group's final preference, even if it would fail on its intrinsic merits without that support. (Sunstein, et al., 2015)

Hence, commanders must exercise caution in directing specific COAs in their initial guidance unless that direction is firmly rooted in imperatives (such as time constraints), or on insider knowledge. To reduce the risk of homogenized thinking among planners, this knowledge may be better passed as specific guidance to the intelligence staff conducting IPB, when resources can be directed to either confirm or discount these early inclinations.

Intelligence Preparation of the Battlefield

As intelligence staffs gather and interpret masses of data to help define the battlespace and key players within, information may arise that *should* significantly alter the direction of planning. Here, OPP guidance from the Canadian Army standpoint deserves emphasis: "[…] ongoing updates to the intelligence picture answer the question '*has the situation changed, and do we need to change our plan?"* (Canadian Army Command and Staff College, 2010). An intelligence operator, in possession of "game-changing" information, faces a group decision-making pitfall, mentioned in Irving Janis' writings as the tendency toward self-censorship. In addition to MARKET GARDEN, consider the early knowledge possessed by members of the US Navy and diplomatic services preceding the Japanese attack on Pearl Harbour on 7 December 1941. In this case, deciphered Japanese messages gave credible evidence that the Imperial Navy was manoeuvring to attack, but it was dismissed by analysts because of their decision to "select[ing] the explanations [for indicators] that fitted the popular hypothesis" (Janis, 1972). Jerry Harvey, in his book *The Abilene Paradox*, takes a more humanistic view, stating that much self-censorship has roots in our own fears of alienation, separation, and ostracism (Harvey, 1988). To that end, it would seem that, without the proper mind-set and training, the intelligence officer could be especially inclined to self-censorship.

Mission Analysis

OPP Stage Two – Orientation – presents another opportunity for the commander to encourage or destroy staff creativity and innovation in advance of COA development. The Commander's Planning Guidance (CPG) issued at the end of mission analysis may shape the mind-set of planners to the detriment of maintaining an objective, broad view of the problem and its potential solutions. Without individuals who feel confident providing professional dissent as the team enters COA development, the judgment of the planning team may become dangerously homogenized (Vore, 2013). The personality of the commander can play a significant role in either avoiding or exacerbating this issue. The famous Field Marshal Montgomery, known for his aggressive leadership style, "knocked down" dissenters and "refused to listen to the exhortations of his headquarters staff" (Houghton, 2015). These personality traits were, according to Houghton, "always likely to give rise to a dysfunctional decision-making process." While this behaviour could also apply to hindrance of creativity during COA development, it is arguably more dangerous here because the suppression of creativity and dissent at this formative planning stage may result in the omission of options that ought to be brought forward at least as far as Stage Three, and a rigorous COA comparison.

The business sector is aware of the dangers of suppressing creativity, and has provided several applicable observations for military planners. Adam Grant, in his Harvard Business Review article, *How to Build a Culture of Originality*, asserts that most individuals are, "in fact quite capable of novel thinking and problem solving, if only their organizations would stop pounding them into conformity.[…] organizations need to strike a balance between cultural cohesion and creative dissent" (Grant, 2016). Many techniques used by corporations are finding their way into military planning. For instance, a planning team from diverse backgrounds, military branches, and ages can help to avoid homogeneity and stereotyped viewpoints. Since the military is already, from a civilian viewpoint, a very homogeneous group of individuals, planning teams could be occasionally "shaken up" to add dissenting points of view (Vore, 2013). Another suggestion, which is contrary to OPP structure, is the notion that supervisors should never speak first (Recall the notion that "the group's conclusion might well be an accident of who spoke first" (Sunstein, et al., 2015)). Individual brainstorming, known as "brainwriting," is a useful technique when individuals are allowed full creative autonomy without the influence of their teammates, then are encouraged to come to the planning session with pre-determined notions as to how to solve the problem (Vore, 2013). From there, constructive dissent and debate should come readily to the group.

Course of Action Development

The amount of staff effort expended in the OPP often hits a crescendo at the point of COA development and selection. Here, the OPP Handbook challenges typical military sentiment that a requirement to change the plan is evidence of planning incompetence, stating, "Adjustment to a plan is not an admission of failure. Failure *will* occur if a plan no longer reflects reality" (Canadian Army Command and Staff College, 2010).

Now, the OPP is again vulnerable to a group decision-making trap, not because of the opinions of the commander, but because the plan has reached a critical level of personal investment in the eyes of the planners. The emergence of plan-altering information late in the process risks being rationalized away, if not by individuals, then by what Janis termed the "mindguard" of the organization (Vore, 2013). Little can be done to prevent this tendency to "fall in love with the plan" from a procedural or leadership standpoint, beyond encouraging a no-blame culture amongst the staff. However, the use of Red Teamers could play an important role as COAs are "fleshed-out" and compared.

Red Teaming is a technique that has been formalized in the US Army for over a decade (Mulrine, 2008). It involves the use of a specially educated third party to observe and challenge the plans and assumptions made by the blue force (Lauder, 2016). Culturally, however, its employment can be challenging. Unless a climate of mutual trust and teamwork is fostered when Red Teamers arrive, blue force members may dismiss it "as a distraction or, even worse, a deliberate attack that unnecessarily consumes much-needed resources in a time of constraint" (Lauder, 2016). It must be clear to both sides that a Red Team's mission is not to derail the process – something to which an overworked staff officer would be especially resistant – but to challenge ways of thinking and points of view. The US Army "Red Team University" encourages its graduates to present arguments and then drop them, leaving the blue force with the final decision to either ignore or act on the divergent idea. Success of the Red Team is illustrated when the blue force incorporates the red teamer's point of view as if it was their own (Mulrine, 2008).

The commander re-enters the planning process at the decision brief, where the staff presents detailed concepts for unique COAs and then offers a recommendation based on a rational comparison method (Canadian Armed Forces, 2008). Again, the military's hierarchical, cohesion-demanding culture may affect the decision-making process. Groupthink theory warns of *mindguards*, whose self-appointed role is to shut out dissenters and present a unified front to the supervisor (Vore, 2013). The behaviour of former US president Ronald Reagan's staff during COA development, which led to an arms deal with Iran – now known as the Iran-Contra Affair – has been described as a "spectacular" example of mindguarding.

Kevin Dougherty's book, *Military Decision-Making Processes*, describes how Reagan's closest advisors shut out dissenters and "fail[ed] to advise him against proceeding 'on a highly-questionable course of action even in the face of [individual] strong conviction to the contrary'" (Dougherty, 2014). This tendency towards positive, unanimous "happy talk," argues Sunstein and Hastie, often occurs around a boss due to a "halo effect." Without some anxious or naturally-critical personalities in the staff, subordinates will tend to assume that "boss knows best" and publicly support a commander's decision, even if it is incorrect and goes against the staff's recommendations (Sunstein, et al., 2015). However, can a military staff afford to have these pessimistic, straight-talking employees that are deemed critical to successful decision-making in the political and business worlds? In *Credit and Blame,* Charles Tilly recounts an interview with the former CEO of General Electric (GE), Jack Welch, who credits his success on his "candor" and ability to make an honest evaluation of performances:

> "From the day I joined GE to the day I was named CEO, twenty years later, my bosses cautioned me about my candor. I was labelled abrasive and consistently warned that my candor would soon get in the way of my career. Now my GE career is over, and I'm telling you that it was candor that helped make it work. […] We gave it to one another straight, and each of us was better for it." (Tilly, 2008)

Arguably, there exists a means by which a subordinate's reservations can find their way to a commander, and that route is typically via the influential chief of staff or deputy commander. However, since the OPP is a command-driven process and the CAF command culture is one that seeks and accepts responsibility for the outcome of decisions made, staffs will frequently be forced to rationalize the conflict between their own convictions and the decisions of their leaders. There is no “silver bullet” in this scenario.

Plan Development and Execution

In a headquarters that has progressed to Stage Four – Plan Development – there exists an understandable atmosphere of “frozen in time” as staff labour to produce detailed direction – an operations order – for their subordinate units before the plan is overtaken by events. Despite the tendency for the HQ to work in an “information vacuum” during this stage, plan wargaming, concept of operations (CONOPS) briefings to higher headquarters, and continuous monitoring of the situation all offer opportunities for staffs to recognize and correct shortfalls. The groupthink phenomena and other group decision-making perils potentially at-play in Stage Three are applicable in Stage Four; they will not be re-introduced here.

Risk, however, is a topic that deserves attention as a headquarters and its commander enter the execution phase of the OPP. The CAF uses a probability/severity model and five-phase risk-management process that is common in NATO and the business world (Canadian Armed Forces, 2007). What is lacking in Canadian doctrine, however, is the acknowledgement that risk analysis may fall victim to unhealthy group dynamics. In its principal risk-management publication, *Risk Management for CF Operations*, the CAF does not note a well-documented phenomenon whereby members tend to accept, based on group norms, a higher (occasionally lower) level of risk in a group setting than they normally would have accepted as individuals. This tendency, sometimes called “groupshift” or “risky-shift,” can be summarized as a group’s inclination toward more risky behaviour and decisions thanks to the shared, diffusive effect of being in a group, where individual responsibility may be shirked (Smit, 2007). Whether this theory is valid in a military setting, where commanders are taught that they alone must accept operational risks, is open to question. However, it has been suggested that the detailed, immersive planning and problem familiarity that characterizes OPP can also lead to a reduced perception of the risks involved. This, coupled with the confident, self-assured nature expected of commanders, may lead to increased risk-taking behaviour in its own right (Knighton, 2004).

To balance the argument that military leaders may tend to accept greater risk in operations due to groupshift in the risk assessment process, one must consider the western societal and political pressures facing commanders, and a near-zero tolerance for making mistakes. Examples of modern-day military risk-aversion based on political and public expectations of perfection are plentiful and while, in the author's view, no "blame culture" exists in the CAF, the way society views military mistakes plays a significant role in hindering what Nathanial Fast calls "a culture of psychological safety" in what ought to be an innovative, risk-taking organization (Fast, 2010). Jerry Harvey devotes a chapter to the concept of grace in response to mistakes, explaining that the US military prescribes to a "doctrine of zero defects" which ultimately destroys the career of any officer who makes a serious mistake (Harvey, 1988). Unquestionably, the fear of making a career-ending mistake would temper the risk tolerance of all but the most reckless commanders in operations short of war.

Conclusions

The pitfalls of group decision-making may manifest themselves in all steps of the operational planning process and, beyond some sage warnings in our OPP handbooks, there are no built-in safeguards to assist planners in identifying groupthink and defending against it. Military history is replete with examples of how military decision-making processes have failed due to the perils of group dynamics. Discussion of these phenomena, from a military/leadership psychology standpoint, must occur when training decision-makers and planners. Some recommendations include:

1. Educate staff on groupthink. Despite its detractors, the indicators based on Janis' theory remain valid enough to make staff members aware of group decision-making challenges in general terms.

2. Be wary of over-prescriptive planning guidance during the initiation stage. Suggest that early inclinations may be better directed as a point of exploration

during IPB. Likewise, be aware of the dangers of restricting creativity in COA development through the CPG.

3. Consciously amend planning team composition to break homogeneity and encourage productive dissent. Introduce other ranks, military trades, services, or Defence Civilians into the process when appropriate.

4. Consider adding some groupthink checks into the OPP. Add a friendly factor: *own biases?* Deliberately re-evaluate the situation at regular intervals, in spite of the urge to "fight the plan."

5. Have a dedicated, properly trained Red Teamer join the staff to provide a fresh, productive dissenting view. The deputy commander or chief of staff is too encumbered by their principal duties to fill this role effectively.

6. Help create a military decision-making culture that emphasizes the training environment as a "safe zone" to take appropriate risks. Use civilian business practices to encourage creativity and innovation amongst staff and understand the possible effects on risk perception due to groupshift and familiarity with the plan.

7. Lastly, reward professional, productive dissent from staff members at the appropriate time. At the very least, do not punish it.

During any planning process, whether collective or individual, time and resource constraints may lead to "wishing-away" factors that would cause impediments to the plan. While this may seem unconscionable, one must consider the effects of this and other groupthink indicators, particularly the effects of self-censorship, and their role in flawed decision-making. Additionally, the commander must remain conscious of their potential part in a poor group decision-making dynamic, since the operational planning process simply does not have the safeguards built-in to mitigate these hazards. Ultimately, an educated commander and staff is the best defence.

Bibliography

Canadian Armed Forces. 2007. *CF Joint Doctrine Manual - Risk Managment For CF Operations.* Ottawa : Department of Defence, 2007.

—. 2008. *CF Joint Publication 5.0 - The Canadian Forces Operational Planning Process.* Ottawa : Department of National Defence, 2008.

—. 2007. *Command in Land Operations.* Ottawa : Department of National Defence, 2007.

Canadian Army Command and Staff College. 2010. *The Operational Planning Process Handbook.* Kingston, ON : Department of National Defence, 2010.

Dougherty, Kevin. 2014. *MIlitary Decision-Making Processes - Case Studies Involving the Preparation, Commitment, Application and Withdrawal of Force.* Jefferson, NC : McFarland and Company, Inc., 2014.

Fast, Nathanael J. 2010. How to Stop the Blame Game. *Harvard Business Review.* [Online] May 13, 2010. [Cited: September 22, 2017.] https://hbr.org/2010/05/how-to-stop-the-blame-game.

Grant, Adam. 2016. How to Build a Culture of Originality. *Harvard Business Review.* [Online] March 2016. [Cited: September 22, 2017.] https://hbr.org/2016/03/how-to-build-a-culture-of-originality.

Harvey, Jerry B. 1988. *The Abilene Paradox and Other Meditations on Management.* San Francisco, CA : Jossey-Bass Publishers, 1988.

Houghton, David P. 2015. Understanding Groupthink - The Case of Operation Market Garden. *Thinking Strategically - US Army War College Strategic Studies Institute.* 2015, 10.

Janis, Irving L. 1972. *Victims of Groupthink - A Psychological Study of Foreign-Policy Decisions and Fiascoes.* Boston, MA : Houghton Mifflin Company, 1972.

Knighton, Wing Commander R.J. 2004. The Psychology of Risk and its Role in Military Decision-Making. *Defence Studies.* 2004, Vol. 4, 3.

Lauder, Matthew A. 2016. The Black Art of Red Teaming - 15 Axioms. *Canadian Army Journal.* 2016, Vol. 17, 1.

Mulrine, Anna. 2008. US News. *The Army Trains a Skeptics Corps to Battle Groupthink.* [Online] May 15, 2008. [Cited: September 15, 2017.] https://usnews.com/news/world/articles/2008/05/15/the-army-trains-a-skeptics-corps-to-battle-groupthink.

Ryan, Cornelius. 1974. *A Bridge Too Far.* London : Hamish Hamilton Limited, 1974.

Smit, Pieter J. 2007. *Management Principles: A Contemporary Edition for Africa.* Cape Town : Juta & Co. Ltd, 2007.

Sunstein, Cass R. and Hastie, Reid. 2015. *Wiser - Getting Beyond Groupthink to Make Groups Smarter.* Boston, MA : Harvard Business Review Press, 2015.

Tilly, Charles. 2008. *Credit and Blame.* Princeton, NJ : Princeton University Press, 2008.

Vore, Keith. 2013. Understanding Groupthink. *Small Wars Journal.* [Online] April 8, 2013. [Cited: September 22, 2017.] http://smallwarsjournal.com/print/13970.

Can small powers have grand strategies? MAJ Vitalijus Anisimenko

Introduction

411 BC the great Greek historian Thucydides depicted the international political thought of particular time by stating that the “dominant exact what they can and the weak concede what they must“ (Thucydides, 2009 (first published 411 BC), p. 302). Today the international order seems to have progressed enough, to guarantee options for both weak and strong. But is it really so, or do we still live in the world where the might is right? Different definitions of a small state[1] and Grand Strategy give a basis for a discussion whether a small state can have Grand Strategy at all. Contrary to the realist understanding, the flourishing wave of institutionalism, especially after the end of the Cold War, has facilitated Grand Strategic options for multiple small states. This essay argues that the deterioration of global security situation in recent years and possible consequent transformation of World order is likely to deprive small states of “borrowed” power on which their Grand Strategies were based. Depending on the level of threat of their geopolitical setting, small states might eventually realize that the combination of their innate military, economic and soft powers is not enough to sustain their Grand Strategy. This work will initially review the concepts of small state and Grand Strategy. Later the elements of power of the state will be examined in the light of most influential paradigms of international relations: realism and institutionalism. The conditions provided by different elements of power to construct and sustain a Grand Strategy for a small state will be analysed using the case study of Iraq.

Small state

The starting point of the discussion on the availability of Grand Strategy to a small state begins with the discussion on what a small state is and from where it draws its power. From the perspective of the realism, a power of a state is seen as a possession

[1] A small state is regarded as a small power.

and is measured in relative terms compared with the opponent's power. A small state is seen as one having less power in the face of a larger state and thus being unable to change the relationship between the states by itself (Wivel, Bailes, & Archer, 2014, p. 7).

The rise of international institutions after World War II strengthened the institutionalist thought. The emergence of the unipolar world after the end of Cold War and the collapse of the Soviet Union in 1991, the integration of European Union and globalization fostered international relations and reduced possible threats in the geopolitical environment. Then, the power of a state was defined as something that the state exercises in its relationships with other entities rather than possesses (Mouritzen & Wivel, 2005, p. 6). The application of power was examined in connection to the construct of the international system rather than in relation to a specific opponent. The emphasis from the elements of hard power shifted to the effectiveness of exercise of non-military and especially soft power in the international environment. Accordingly, small states were defined as being the weaker subject in an asymmetric relationship without the capability to transform the character or functioning of the relationships at the systemic level by itself (Mouritzen & Wivel, 2005, p. 4).

In fact, as seen from definitions above, no quantitative indicators can define which states are small. The smallness is contextual, tied to an existing geopolitical situation (Molis, 2006, p. 80) and therefore the same state can be regarded differently in different settings. The paradigms of realism and institutionalism agree on the essential function of a power of a state to influence other states in pursuing its interests. The difference belongs to the matter what generates the power for a state and to what extent peace and cooperation is a viable option in the anarchic system. Rather pessimistic realists emphasize competition and war and appreciate only the innate sources of power that the self-reliant state is able to independently control even in the face of military threat. At the same time, optimistic institutionalists assume security situation as being relatively stable. They emphasize the effect of institutions in international cooperation, which boosts the power of small states in particular. In this case, power is not necessarily possessed and thus is not always controlled independently by the state it benefits.

Grand Strategy

The universally agreed definition of Grand Strategy, just like the definition of a small state, is a non-existing subject. It has evolved alongside with the military and political thought. Barry Posen describes modern realist definition of Grand Strategy as “a state’s theory about how it can best ‘cause’ security for itself”. He states unambiguously what the core of the Grand Strategy is – the survival of the state. He further explains, “a Grand Strategy must identify likely threats to the state’s security and it must devise political, economic, military and other remedies for those threats.” (Posen, 1984, p. 13). Paul Kennedy reflects institutionalist thinking of Grand Strategy as he defines it as at least 20 years ahead looking policy of the state on the use of all available military and non-military means of power to promote or sustain long-term wartime as well as peacetime interests (Kennedy, 1991, p. 5). Here the aims of Grand Strategies can differ as they depend on the geopolitical context and might possibly include objectives unrelated to survival. Therefore, the definitions of Grand Strategy and a small state conflict when viewed from different paradigms. What might be a Grand Strategy for an institutionalist is not necessarily a Grand Strategy for a realist. At the same time, what a small state is for a realist might not be a small state for an institutionalist. Thus the answer to the question whether a small state can have a Grand Strategy depends on a perspective from which you answer the question.

This essay will assume both definitions are viable depending on the context they are used in. It is useful to analyse the function of military, economical and soft powers of a state as the key elements of state power (Nye S. J., 2011, pp. 25-109) in different situations. Such analysis will help determine the usefulness of different paradigms for judgement on small state’s ability to have Grand Strategy in different circumstances.

Military power

Military power gives possibility to compel, coerce or deter the opponent if security is at stake. Using institutionalist approach small states often take advantage of joining particular organisations like NATO or the UN to augment their existing military power and secure their survival. This brings them a comforting effect by providing an often-false sense of strong backing in case of military threat. Realists state, that military power, which, when used in concert with other elements of power, is a prerequisite of Grand Strategy (Hart, 1991 (first published in 1941), p. 322). Contrary to institutionalist approach, realists maintain, that military power cannot be “borrowed” through membership in the alliance. For them, unlike in economic matters, security of a state is an issue, which cannot be trusted to be solved by another state as the risk of abandonment, and thus the decisive defeat, is impossible to mitigate (Mearsheimer, 1995, p. 19).

In the last quarter of the 20th century, Iraq was one of the regional powers in the Middle East. It struggled with transportation of oil through the main artery of Shatt al-Arab waterway as it was shared with its regional rival Iran (Frankopan, 2015, pp. 457-488). The latter, being a stronger side and US ally during the most of the 1970s, refused to pay agreed price for the use of Shat al-Arab waterway to Iraq. It also attempted to destabilize Saddam Hussein regime by empowering Iraqi Kurds in their attempt to secede from Iraq. In 1979, Iranian revolution brought Ayatollah Khomeini to power. Unlike the previous ruler, he expressed a strong anti US sentiment what significantly aggravated the US-Iran relationship. The US felt Iran slipping out of its hands and saw the conflict between Iraq and Iran as a possibility to compel Iran to resume cooperation (Frankopan, 2015, p. 482). Consequently, the US encouraged Iraq to attack Iran, supported financially and influenced its allies to support Iraq with military equipment to sustain war against Iran (Jensen & Klunder, 2001, p. 5). Saddam Hussein engaged in, as he thought, a short limited war to preserve power, seize oil-rich Khuzestan province and gain unrestricted access to the waters of the Persian Gulf. This would have served as a catalyst to Iraqi oil export and facilitated the rise of Iraq above other regional rivals. Saddam Hussein took the US support as a backing while the US played a double game. After resuming the negotiations with Iran, the US went forward to cement reborn relationships. Starting from 1985, it initiated shipments of arms to Iran through Israel and ensured neither side was able to win (Yetiv, 2008 p. 57). The war lasted eight years - far longer than estimated by Saddam Hussein and it did not bring desired effects. The failure to identify true US objectives behind the support served a blow to the Iraqi strategy.

As shown above, foreign military support ranging from unofficial supply of armament to collective defence agreements, supplement military power of a small state. Nevertheless, this support is extremely hard to prevent from withdrawing. As put by Thomas Hobbes - “covenants, without the sword, are but words“ (Hobbs, 1981 (first published 1651), p. 111) and small states simply have no swords. History tracks back instances when alliances had decisive importance by providing only short-term security from external threats of greater powers (Hart, 1954 (first published in 1941), p. 25). Unfortunately, alliances consist of individuals from different cultures having different war aims, political perceptions and worldviews. These more often than not result in conflict with their allies (Hart, 1954 (first published in 1941), p. 28). Therefore, great powers remain in alliances and support small states militarily as long as there is a strategic interest in doing so. The withdrawal of support leaves the military power of small state insufficient for independent influence over the opponent of greater power and thus results in a collapse of a Grand Strategy of a small state.

Soft power

Culture, political values and policies are the primary currencies of soft power (Nye, 2011, p. 99). Both, the school of realism and institutionalism recognize the effectiveness of it. Culture, if effectively demonstrated, facilitates attractiveness. Shared values and policies create conditions for small states to become members of international institutions. Using the voting system in those, small states enhance their security and gain influence. Influence is further augmented by creating an image of a relevant partner through side-lining with the policy of great powers, providing or facilitating solutions to commonly recognized issues and impartially mediating disputes (Wivel, 2009, p. 10). International institutions often benefit small states even more than great powers. International institutions create common rules of behaviour regardless of inequality of power of its members and thus make hard power less important. They formalize the acceptable behaviour of its members, what makes the (mis-)use of power more evident (Wivel, 2009, p. 4). International order is maintained through monitoring and sanctioning the violators of established rules including use and threat of use of force. Nevertheless, institutional binding of great powers, which favours minors, at some point has a potential to fail. If rules of the international institution hamper the achievement of vital goals of great power, the latter might choose to bypass the formal settings. The withdrawal of great powers poses a tremendous risk to international institutions, as without the resources of great powers the rules of institutions are impossible to maintain (Wivel, 2009, p. 5). The soft power influence and protection gained by small states in international institutions has, therefore, its limits. Small states are particularly effective in using their soft power to influence decisions in areas of less importance, while decisions concerning vital issues, especially in security field, are subject to circumstances and, in particular, to the interests of great powers (Steinmetz & Wivel, 2010, p. PXIII).

In mid-1980s, Saddam Hussein clearly saw a risk of losing a war against Iran. Regardless of the fact that Geneva Protocol of 1925 banned chemical weapons, Iraq used them to secure military objectives. Iran, being a member nation of the United Nations (UN), brought out the issue of the use of chemical weapons in 1983 to the Security Council (SC) and sought resolutions on Iraq to terminate the use of those (Frankopan, 2015, pp. 476-477). One would have assumed that Iranian diplomatic effort to seek the UN protection against violation of some of the most elementary norms in international relations would be a perfect example of soft power importance and small states' benefits inherent in the UN organisational arrangement. Yet the reaction of the UN to the call of Iran did not favour the perspective of institutionalists, who claim that, institutions are in capacity to alter state's selfish preferences and, in turn, the policy (Mearsheimer, 1995, p. 13). Instead, the realist thinking proved to be prophetic. According to them, institutions are considered to be "based on self-interest of the great powers" and are not the "determining factor of stability" (Mearsheimer, 1995, p. 13). The UN failed to protect its member. It was only able to pass out resolutions, which condemned violations of international law. No actions were imposed. The US did not demonstrate institutional leadership by distancing itself from its own interests in favour of international law. Although the US did publicly state it was "strongly opposed to the use of chemical weapons" (Frankopan, 2015, p. 476), it did not seek any actions that would have effectively stopped Iraq from using those. As mentioned before, this was the time, when the US benefited from successful Iraqi operations against Iran (Frankopan, 2015, p. 477). By an interesting twist of history, Iraq was at the other side of the table in 2003, when no international law rules were able to prevent the coalition led by the United States from invading Iraq despite missing UN SC resolution enabling such an action. The fate of Iraq in times of great crisis was thus determined by great power interests and not by institutional arrangements favouring soft power approach.

As can be seen, soft power of a small state, amplified by international cooperation, might perfectly facilitate the achievement of strategic economic, environmental or even security-related goals if those are in the interests of great powers. In case the interests of great powers do not match the interests of small states, the soft power of the minor is likely to be insufficient to create a favourable change or maintain preferred status quo in pursuit of its goals and thus sustain a Grand Strategy.

Economic power

Economic power of a state encompasses its natural resources, capital and industry. It provides a capacity to influence other actors via various economic means, ranging from financial support to sanctions (Graham, 2013, p. 1). It ensures the wellbeing and stability of a state and provides "weight" in international relationships. Economic power is enhanced by the effective use of international institutions such as the World Trade Organization, the European Union or others. If the size of economic power of a small state facilitates effective influence over its geopolitical environment and the threat to the survival of the state is not present, robust economy alone might be a solid basis for a state's Grand Strategy. However, if not accompanied by sufficient military potential, the economic power is likely to be insufficient to exercise influence or maintain resilience in the face of adversary.

Iraqi economy was ranked as the most advanced among Arab world countries in the beginning of 1980s. It was built primarily on the revenue of oil, but also had a significant industry, well-functioning transport system and relatively good infrastructure (Sanford, 2003, p. 1). The foreign reserves reached 35 billion USD. The economy ensured a substantial middle class, effective education and health systems. As Iraq purchased arms from the Soviet Union and was in competition with Iran, its policy was not in line with the US, which is the greatest contributor to the World Bank and the International Monetary Fund. Despite Iraqi economic potential, and with no sanctions in place, International Monetary Fund and the World Bank provided little assistance to the Iraq (the World Bank financed the last project in 1973 (The World Bank, 2018)). In the course of Iraq-Iran conflict, Iraqi economy did not provide economic options to influence Iran. To pursue strategic aims, Iraq transformed its economic power to military by spending up to 102 billion USD on arms purchases in 1980s alone (Sanford, 2003, p. 4) (Graham, 2013, p. 2). Despite the effort, it proved to be insufficient to produce victory due to similar economic potential of the opponent and the influence of the US, which repeatedly changed sides it supported during the conflict (Frankopan, 2015, p. 482). The support of the International Monetary Fund and the World Bank became available to Iraq only after the removal of Saddam Hussein regime (International Monetary Fund, 2018) (The World Bank, 2018).

In comparison, the UN economic sanctions, which were imposed after Iraq had attacked Kuwait in 1991, provide a proof of the effectiveness of economic means if a superior against the weaker uses them. Together with debts, which resulted from loans and reparations, sanctions brought Iraqi economy to misery, as by the time the UN sanctions were lifted in 2003, Iraq had the World's highest debt to GDP (Sanford, 2003, p. 15). The destroyed Iraqi economy did not facilitate the change of the regime, which supposedly was the ultimate goal of the UN, but effectively prevented Iraq from posing a military threat to neighbouring countries.

Probably, Iraqi economy in the 1980s would have been a sufficient foundation for Grand Strategy if the latter would only have to ensure the well-being of the state. Meanwhile, Iraqi Grand Strategic aims were security oriented. Deprived of support from international economic institutions dominated by the Western great powers, Iraq only had access to foreign loans from other sources. Even with those, Iraqi economy was insufficient to facilitate the transformation of the balance of power, compel Iran and bring the desired strategic ends. Thus even if the limited economic prosperity of a small state might be sufficient in peaceful times, in time of war it proves unable to support war efforts to a necessary level without the help of great powers.

Conclusion

So, can small states have Grand Strategy? Effective use of a combination of state political, economic and soft power enables small states to pursue their goals depending on the geopolitical environment. One could get mistaken thinking that modern institutionalised world order is a guarantee of Grand Strategic success for all states regardless of their size. Institutions proved to be effective when important issues were not at stake. Thus, small states can only have a Grand Strategy as far as they do not have to bother about their survival. As said by Carl von Clausewitz "in strategy everything is very simple, but not on that account very easy" (Clausewitz, 1989 (first published 1832), p. 178). The most difficult part is the sustainment of the chosen strategy. Understanding whether a state has a capacity for that allows judgement whether constructing the Grand Strategy is worth the resources and time. If a geopolitical context of the state includes military threat, wearing rose-coloured glasses of institutionalism can have disastrous consequences. If a survival of a state is threatened, one should think of the Grand Strategy from the realist perspective. Alliances are not long-term remedy and thus can only be a milestone on the road to the Grand Strategic end. Cessation of being small by maximizing power internally to achieve comparative power balance vis-à-vis the opponent is the most effective security guarantee.

Bibliography

Clausewitz, Carl von. 1989 (first published 1832). *On war.* [ed.] Michael Howard and Peter Paret. Princeton: Princeton University Press, 1989.

Frankopan, Peter. 2015. *The Silk Roads: A New History of the World.* London: Bloomsbury, 2015.

Gaddis, John Lewis. 2009. American Grand Strategy after War. *What is Grand Strategy?* Durham: Duke University press, 2009.

Graham, James. 2013. Military Power vs Economic Power in History. *On This Day.* [Online] 3 September 2013. [Cited: 26 March 2018.] https://www.onthisday.com/world/power.php.

Hart, B. H. Liddel. 1991 (first published in 1941). *Strategy.* London: Plume, 1991 (first published 1941).

Hobbs, Thomas. 1981 (first published 1651). *Leviathan.* London: Penguin Books, 1981 (first published 1651).

International Monetary Fund. 2018. International Monetary Fund. *Iraq: Transactions with the Fund.* [Online] 2018. [Cited: 26 March 2018.] http://www.imf.org/external/np/fin/tad/extrans1.aspx?memberKey1=460&endDate=2018-01-31.

Jensen, Kurtis and Klunder, Matthew. 2001. *Saddam Hussein's Grand strategy during the Iran-Iraq war.* Washington: National War College, 2001.

Kennedy, Paul (ed.) 1991. *Grand strategies in war and peace.* New Haven: Yale Univercity press. 1991.

Mearsheimer, J. Jonh. 1995. The false promise of international institutions. *International Security, Vol. 19, No. 3.* 1995.

Molis, Arūnas. 2006. The Role and Interests of Small States in Developing European Security and Defence Policy. *Baltic Security & Defence Review Volume 8.* 2006.

Mouritzen, Hans and Wivel, Aleksander. 2005. *The Geopolitics of Euro-Atlantic Integration.* Abdington: Routledge, 2005.

Nye, S. Joseph. 2011. *The future of power.* New York: PublicAffairs, 2011.

Posen, Barry. 1984. *The Sources of Military Doctrine: France, Britain and Germany between the World Wars.* Ithaca: Cornell University Press, 1984.

Sanford, Jonathan E. 2003. *Iraq's Economy: Past, Present, Future.* s.l. : Congressional Research Service. The Library of Congress, 2003.

Steinmetz, Robert and Wivel, Anders. 2010. *Small states in Europe. Challenges and opportunities.* Abdington: Routledge, 2010.

The World Bank. 2018. The World Bank. *The World Bank. Projects & Programs.* [Online] 2018. [Cited: 23 March 2018.] http://www.worldbank.org/en/country/iraq/projects

Thucydides. 2009 (first published 411 BC). *The Peloponnesian War.* Oxford: Oxford University Press, 2009 (first published 411 BC).

Wivel, Anders. 2009. *The Grand Strategies of Small European States.* New York conference proceedings, 2009.

Wivel, Anders, Bailes, Alyson J.K and Archer, Clive. 2014. *Setting the scene: Small states and international security. Small States and International Security: Europe and Beyond.* Abdington: Routledge, 2014.

Yetiv, Steve. 2008. *The Absence of Grand Strategy: The United States in the Persian Gulf, 1972–2005.* Baltimore: Johns Hopkins University Press, 2008.

Is the network theory the most suitable for understanding terrorist radicalisation? MAJ Deimantas Čyžius

’Kill one, terrify a thousand’
Sun Tzu

Introduction

On the 17th August 2017, a van drove into the pedestrians on Las Ramblas Street Barcelona, Spain and killed thirteen people. More than one hundred people were injured. The radical Jihadi terrorist group assumed responsibility for the attack. ‘Jihadi terrorism is a highly complex and constantly changing phenomenon, which makes headlines on a daily basis and stands at the forefront of national and international agendas’ (Bakker, 2006, p. 5). European countries face challenges from unpredictable Jihadi movement in order to effectively implement counter-measures against more radical terrorism and ensure security. Jihadi terrorist groups are using increasingly new methods and tactics, which no longer require huge resources for committing an attack. Many researchers try to explain the complexity of radical behaviour and study terrorism through the social networks’ and movements’ viewpoint.

Therefore in this essay, the main focus will be on Jihadi terrorism analysis through the social networks that deal with terrorists’ social relationships and interaction in order to better understand terrorism radicalization. The radical terrorist groups operate as networks, where members are connected with different nodes, links and have all appropriate attributes of social networks. According to Ressler (2006, p. 12), ‘the social network analysis provides important information on the unique characteristics of terrorist organizations, ranging from issues of network recruitment, network evolution, and the diffusion of radical ideas’. Is it possible to understand why terrorism becomes more radical and how the European countries can timely identify threats and effectively implement counter-measures for preventing possible terrorist attacks? There is no unique answer to the question, what makes individuals join terrorist groups and how radicalization could be suppressed in the European region. Although radicalism is widely spread within extremist terrorist groups, whose members are integrated into the social networks, various theories explain the radical terrorists' behaviour from different perspectives.

This essay will argue, that the network theory is not the most suitable for understanding Jihadi terrorism radicalization on its own, but provides effective methods to identify radical Jihadi terrorists within social networks and implement relevant counter-measures to increase European regional security. This paper is divided into three chapters. In the first chapter term 'radicalization' will be defined as a process of transition from nonviolent to radical extremism, which is the most recognizable attribute of Jihadi terrorist groups. The second will explain how different theories are interconnected and support each other in understanding the terrorists' radicalisation. And the last chapter will give the overview of how the network theory contributes to European security institutions, agencies in identifying and countering radical terrorism threats. Finally, the conclusions will be made and the main essay's question answered.

Radicalization

The term 'radicalization' is widely used in the research of the Jihadi terrorism, but still poorly defined and is often confused with 'extremism'. Terrorists conduct violent attacks within a different environment and use various radical methods in a particular context that shows the complexity of terrorism 'radicalization'. Randy Borum (2011, p. 30) defines 'radicalization' as 'the process of developing extremist ideologies and beliefs' where individuals are engaged in violent terrorist actions. According to Olesen (2009, p. 8) 'radicalization' is 'the process through which individuals adopt violent strategies – or threaten to do so – in order to achieve political goals'. Other two researchers McCauley and Moskalenko (2008) define 'radicalization' as characteristic of group dynamics. According to them radicalization is 'increasing extremity of beliefs, feelings, and behaviours in directions that increasingly justify intergroup violence and demand sacrifice in defence of the in-group' (McCauley and Moskalenko, 2008, p. 415).

Therefore 'radicalization' is understood as a process in which groups' or individuals' beliefs and attitudes become more extreme in political, social and religious spheres. This process gives an understanding of individuals and groups behaviour within society and radical organizations and shows how people become a part of violent terrorism and conduct radical actions. Also, it is important to notice that different states (Holland, Denmark, United Kingdom) security services which fight against terrorism understand ‘radicalization’ in a more narrow way and explain it as ‘a use of undemocratic or violent means to reach a specific political/ideological objective’ (PET, 2009, p. 1). Their focus is more on the identification of objectives such as terrorist groups and individuals in order to effectively counter possible terrorist threats.

Jihadi terrorist organizations such as Al Qaida and The Islamic State of Iraq and Syria (ISIS) are very good examples of terrorism ‘radicalization’. These organizations have a unique political narrative, ideology and still, attract new members or supporters. All over the world, there are thousands of Muslims who support Jihadist movement, but themselves are not engaged in terrorism. It shows that often ideology is not connected with actions. From the perspective of the national security, it is important to identify the clear criteria of extremist ideologies which brings a real threat, and which do not conduct violent actions. There is still an open discussion between countries, which implement counter-terrorism measures that for identification of real threat there is a need to expand the focus from the radical violent actions to the nonviolent extremism because the distinction between them is unclear. Usually, the most radical Jihadi groups use approach towards extremism as Peter Neuman explains. According to Neuman (2010, p. 12) ‘extremism, can be used to refer to political ideologies that oppose a society's core values and principles’. This approach is widely applied to ideology with religious supremacy and where the core democratic principles and human rights are opposed. Let’s analyze how the radical behaviour is explained by different research theories.

Network theory vs other theories

Since the late 1960s, many researchers tried to answer the question, why people join radical terrorist’s groups and conduct violent actions. Analysing terrorist groups’ activities, internal relationship, individual behaviour, and external communication, researchers explain the causes of radical behaviour through the different theories. In this chapter network theory, social movement and social psychology theories will be briefly introduced in order to better understand radicalization phenomena and to see similarities and differences between the theories.

The network theory is introduced through the social networks study, where the social relations between groups and individual actors influence radical behaviour. Researchers Knoke and Yang (2008) define network theory through the social network analysis, which uses various methods to study relations among individuals. In this context, Jihadi terrorist organizations are composed of different networks that affect their members' attitudes and behaviour. Marc Sageman (2004, p. 137) confirms that Jihadi terrorist organizations are social networks in which participants act not as 'atomized individuals, but actors linked to each other through complex webs of direct or mediated exchanges'. Network theory concentrates on the terrorist groups' organizational structure, linkage of the members, decision making and recruitment. According to Martin Bounchard (2015), the network theory methods provide unique opportunity to map and analyse the social ties within groups, identify the connections among individuals and understand how they behave. It also provides understanding about internal and external communication, social structure and group values. That gives the accurate view of how terrorist groups function.

The network theory is criticised by Martin Kilduff and Wenpin Tsai (2003), who argue that this theory is not a unique approach, but a collection of methods which are widely used in other theories, such as social psychology, social comparison or balance theories. The network theory is not a single theory, which provides algorithms and concepts on how the actors within a group or a network are structured, related to each other, how the decision-making process is executed towards desired end state and achieved by individuals or groups. Such structures are well recognized in Al Qaida and ISIS terrorist organizations. Critics also argue that in the network theory there is nothing distinctive from other theories and it does not explain the personal reasons why individuals become a part of the network or terrorist organization and why they conduct radical violent actions. Despite the fact, that network theory is still the object of the scholar's debates, its biggest value is that it focuses more on network structure, relationship and links with other groups or individuals.

Looking to the essence of Jihadi terrorist group's radicalization, it is important to comprehend reasons of individuals' radical and violent behaviour. Marc Sageman (2004) provides an explanation why individuals join radical terrorist groups through the analysis of terrorists' common social background and psychological aspects. His research provides evidence that terrorists come from different social groups, countries, and refutes the common stereotype of poor, uneducated, naïve, easy to brainwash terrorist group's members. Terrorist leaders usually are well educated in the Western countries educational institutions and have clear personal motives of involvement in radical movements. Sageman (2004) gives an explanation that terrorists' education and inferior social status are not the reason for violent actions, neither is poverty or madness. Also, terrorists' committed violent actions are not influenced by mental disorders and psychiatric problems. Only a small part of researchers' empirical data confirm facts of mental disorder by conducting cruel acts related to the separate individuals, but not to the whole terrorist group. Generally, it is agreed that radicalization within Jihadi terrorist groups is not caused by a pattern of mental illness and terrorists are normal actors with appropriate mental health. In the network theory studies, the social and psychological factors are limited and do not clearly explain personal motives of joining the terrorist network and support for radical ideas or conduct of violent actions.

The network theory does not analyse the influence of ideology on individuals' radical behaviour. Following the unprecedented attacks by Al Qaeda group, especially from autumn 2001, Al Qaeda ideologically became a symbol which united likeminded Muslim radical groups around the world. Some of them joined Al Qaeda or so-called 'Al Qaeda's' subsidiary groups (Islamic Jihad Union, Fatah al Islam, etc.). Thus, in a very short time, Al Qaeda as a physically existing network became a psychological support for Muslim radicals (Khosrokhavar, 2004). Randy Borum (2010, p. 5) affirms, that 'radical extremist groups and many prospective terrorists find not only a sense of meaning but also a sense of belonging, connectedness and affiliation'. The same model was used to develop ISIS. One of the reasons why ISIS became more radical extremist group than Al Qaeda, is because of individuality, which distinguishes both organizations by their objectives and exclusive behaviour. The ideological background within Jihadi groups, which transmits radical ideas provides a sense of meaning and justifies atrocious behaviour. There are more aspects of radical behaviour, which are not the subject of the network theory. Therefore, to better understand terrorism radicalization, let's analyse the social movement theory research elements.

The social movement theory is defined as ‘a set of opinions and beliefs in a population, which represents preferences for changing some elements of the social structure and/or reward distribution of a society’ (Zald and McCarthy, 1987, p. 24). Jihadi organizations have all elements of social movement and their behaviour is affected by common values and beliefs. The characteristic feature of all radical movements is to ensure their survivability by accepting new members and expanding the group’s influence and capacity. Research on social movements explains the importance of recruitment and employment of new members and focuses on the overall process of violent behaviour. The key aspect of violent behaviour is the persuasion of new members to do radical actions. The recruitment process is focused on the involvement of new members and enlargement of the terrorist network, where members have similar beliefs. Dalgaard-Nielsen (2008, p. 6) confirms that social movement brings understanding on how the solutions, decisions are made within a group and ‘provide motivational frames to convince potential participants to become active’.

Furthermore, a widely discussed attribute of radical behaviour is grievances. The social movement is constructed from individuals and groups, who are not satisfied with the existing situation and seek changes of existing status quo. Jihadi terrorists are convinced that societal injustice morally justifies their violent actions. Quintan Wiktorowicz (2005, p. 3) argues that ‘grievances are generated by socio-structural, economic, and political strains and crises which produce psychological distress and prompt individuals to participate in collective action’. Individuals join radical groups because of personal crisis in which they experience humiliation and discrimination, and personal grievances force them to revenge. In this situation individuals’ view of the world becomes vulnerable and radical ideologies or movements are seen as an opportunity (Wiktorowicz, 2005). The grievances have become a manipulative tool in the process of new members’ socialization and ideological training, which prepare them to conduct violent actions. Research of social movements and networks does not detail on the psychological aspects of radical behaviour, therefore social psychology theory view should be also introduced.

Social psychology research explains how group influence feelings, thoughts and behaviour of group’s members and provides an overview of intergroup dynamics. The social psychology experts McCauley and Segal (1987) explain, that within the groups, individuals act violently, because of the group attitudes and tolerance of radical behaviour. Individuals do not feel personal responsibility and guilt for their actions (McCauley and Segal, 1987). Jihadi terrorist organizations accept violent behaviour and promote the feeling that all radical actions are done for higher goals, which are usually sustained with religious beliefs. The announced global Jihad by radical terrorist groups and struggle with irreligious actors justify all violent actions and used means.

Moreover, the competitiveness between different terrorist organizations is the cause of radicalization (McCauley and Segal, 1987). By conducting more radical actions terrorist groups demonstrate their commitment and higher devotion. That gives more attraction for new members to join the particular terrorist group. The founder of ISIS Abu Musab al-Zarqawi created a faction within Al Qaeda group and started to compete against former Al Qaeda's leadership, because of influence and ideological frictions. This struggle escalated the extremity and more radical behaviour among Muslim world. ISIS became a 'trademark' of the most violent and radical terrorist group within the Middle East and European region. ISIS implemented very effective information campaign by using the internet and media, where depicted violence as one of the most important element of its radical strategy (Stern and Berger, 2015). Social networks are still used for amplification of supporters and acceptance of new Jihadi fighters. Existing tremendous terrorist networks, also rising numbers of radical terrorist groups' supporters and conducted violent attacks became a real challenge for many European countries' security.

Network theory as a solution to a terrorist challenge

The identification of potential Jihadi terrorists within social networks and the most opportune disruption of the network remains the main goal of the law enforcement agencies. The network theory provides effective methods to identify Jihadi terrorists within social networks and implement relevant counter-measures. Mark Sageman (2004) presented important arguments for use of network analysis in the research of terrorism. Understanding the dynamics of terrorist organizations, social influence provides a knowledge how individuals become involved in the terrorist groups and contribute to the mapping of the networks. The biggest challenge according to Sean Everton (2012) is to get access to the network data before violent action is conducted.

Identification and neutralization of the key actors, known as key nodes in the network, or disruption of the links, could decrease the overall efficiency of the terrorist network and even make it dysfunctional. It also helps to improve existing counter-terrorism strategies, action plans and measures.

Since 2004, radical terrorists' networks sprawled in Europe and more Jihadist's attacks were plotted and conducted in the region. According to Sam Jones (2016), European law enforcement and intelligence agencies were struggling to get grips with. From 2014 ISIS started very actively implement terrorist attacks. More than forty Jihadi terrorist attacks and over one hundred plots were conducted in Europe up to the end of 2017 (Simcox, 2017). The law enforcement agencies agree that Jihadi terrorist networks became more decentralized and hard to counter. Agencies started effectively implementing network theory methods, increasing cooperation between European countries in counter-terrorism that gave positive results. By the end of 2016 more than seven hundred suspects arrested for the involvement into Jihadi terrorism, including religiously inspired (EUROPOL, 2017). The results were achieved by identifying important links and nodes of terrorist groups' members and supporters, also observing recruitment process, relationship and communication within internet in different interaction platforms (Facebook, YouTube, Twitter, etc.). However the new phenomena of lone-actor terrorism in Europe, which is very hard to identify, track and counter still remain on the top. John Sawers, a former chief of British foreign intelligence MI6, confirm that ISIS 'central leadership' gave a strategic direction to its members to take the initiative and if needed make decisions by themselves (Jones, 2016). Raffaello Pantucci (2015) affirms that the lone-actor attacks appeared from the change on Al-Qaeda and ISIS tactics, where the Muslims have been called to commit lone-actor attacks in the Western countries. It means that a lone-actor or small cell terrorism is highly increased. European Union (EU) officials emphasize to 'enhance the coherence and the relevance of the EU counter-terrorism policy architecture with the aim to improve both its formal and material effectiveness' (Policy Department for Citizens' Rights and Constitutional Affairs, 2017, p. 30). Since 2001 EU has implemented a number of counter-terrorism plans, took dozens of counter-measures and is looking forward to enhancing common work and mutual support not only between EU members but with all European countries. The main challenge of relevant information sharing between states' national security agencies, institutions about terrorist networks and radical actors still remains.

Conclusions

In conclusion, 'radicalization' is a process in which violent extremism behaviour of Jihadi terrorist groups or individuals is developed. According to different researchers 'radicalization' process is driven by individual or group social, political and religious convictions, and beliefs, including personal and group motives and goals. Through the lens of different theories: network theory, social movement and social psychology theories, researchers explain why individuals become members or supporters of radical organizations and conduct radical, violent actions. The network theory focuses more on how the terrorist groups' members are connected into the networks and provides a valuable understanding of terrorist networks structure and relationship but do not concentrate on members' personal motives of joining the radical networks. In addition, it does not clearly explain the reasons why individuals and terrorist groups become more radical and conduct violent actions. Researchers have found many examples of individuals who became members of radical terrorist groups, support radical, violent extremist ideas and do not conduct violent actions. Such behaviour is determined by internal reasons and personal motives and is better explained through the psychological aspects, social interaction and influence, research of which is objective of social psychology. Social movement theory provides the motivational frame of employment of new members into radical terrorist groups and explains groups' behaviour dynamics. It also shows how radical ideology justifies violent behaviour and complements the other mentioned theories' understanding the radicalization. And the clear answer to the main essay question is that the network theory is not the most suitable for understanding terrorism radicalisation, but together with other theories are supporting each other in radicalisation research.

A better understanding of terrorist organizations is an essential element in the development and implementation of effective counterterrorism strategies used by states' security organizations. The network theory provides very good methods of mapping terrorist organizational structures, it also helps to understand decision-making process and network sustainment. These elements could be effectively countered using operational means and methods. But it must be assumed that the fight against Jihadist ideology should be as important and active as an operational struggle. Complementing counter-measures with methods proposed by other research theories and effective use of means to combat terrorism could be more efficient. Further research and the use of different theories could help better understand changing environment in the radicalization of terrorist organizations and improve counter-terrorism strategies.

Bibliography

Bakker, Edwin. 2006. *Jihadi terrorists in Europe: their characteristics and the circumstances in which they joined the jihad: an exploratory study.* Netherlands Institute of International Relations Clingendael, Hague. [Online] December 2006. [Cited: 30 January 2017] https://www.clingendael.org/sites/default/files/pdfs/20061200_cscp_csp_bakker.pdf

Borum, Randy. 2011. *Radicalization into Violent Extremism I: A Review of Social Science Theories.* Journal of Strategic Security. 2011, Vol. 2, 4.

Borum, Randy. 2010. *Understanding Terrorist Psychology*. Mental Health Law & Policy Faculty Publications. Paper 576. [Online] January 2010. [Accessed 12 DEC 2017] *http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1575&context=mhlp_facpub*

Bouchard, Martin. 2015. *Social Networks, Terrorism and Counter-terrorism.* New York: Routledge, 2015.

Dalgaard-Nielsen, Ania. 2008. *Studying Violent Radicalization in Europe I: The Potential Contribution of Social Movement Theory*. Danish Institute for International Studies, Copenhagen, 2008.

EUROPOL. 2017. *European Union terrorism situation and trend report 2017.* European Union Agency for Law Enforcement Cooperation, Hague, 2017.

Everton, Sean. 2012. *Disrupting dark networks.* Cambridge: Cambridge University Press, 2012.

Jones, Sam. 2016. *Intelligence agencies fight to unravel ISIS network in Europe.* Financial Times. [Online] March 27, 2016. [Accessed 11 MAR 2018] https://www.ft.com/content/20152f82-f35c-11e5-96db-fc683b5e52db

Kilduff, Martin and Tsai, Wenpin. 2003. *Social Networks and Organizations: Understanding social Network Research.* London: Sage, 2003.

Khosrokhavar, Farhad. 2004. *Terrorism in Europe.* ISIM Newsletter, 2004, No. 14.

Knoke, David and Yang, Song. 2008. *Social network analysis.* Thousand Oaks, CA: SAGE Publications, 2008.

McCauley, Clark and Moskalenko, Sophia. 2008. *Mechanisms of political radicalization: Pathways toward terrorism.* Terrorism and Political Violence. July, 2008, Vol. 20: p. 415-433.

McCauley, Clark and Segal, Mary. 1987. *'Social psychology of terrorist groups'*. Group processes and intergroup relations: Review of personality and Social psychology. Newbury Park: Sage, 1987. p. 231–256.

Neuman, Peter. 2010. *Prisons and Terrorism Radicalisation and De-radicalisation in 15 Countries.* A policy report published by the International Centre for the Study of Radicalisation and Political Violence (ICSR). 2010.

Olesen, Thomas. 2009. *Social Movement Theory and Radical Islamic Activism.* Aaarhus: Centre for Studies in Islamism and Radicalization, 2009.

Pantucci, Raffaelo. 2015. *Lone-Actor Terrorism: Literature Review*. Countering Lone-Actor Terrorism Series No. 1.

PET. 2009. *Radikaliseringog terror.* Center for Terror analyse (Denmark). [Online] October 2009. [Cited: 16 September 2017] http://www.pet.dk/upload/radikalisering_og_terror.pdf

Policy Department for Citizens' Rights and Constitutional Affairs. 2017. *The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness*. European Parliament, Brussels. [Online] January 2017. [Accessed 14 JAN 2017] http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf

Ressler, Steve. 2006. *Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research.* Homeland Security Affairs. 2006, Vol. II.

Sageman, Marc. 2004. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Simcox, Robin. 2017. *European Islamist Plots and Attacks since 2014 – and How the U. S. Can Help Prevent Them.* The Heritage Foundation. [Online] August 2017. [Accessed 11 MAR 2018] https://www.heritage.org/europe/report/european-islamist-plots-and-attacks-2014-and-how-the-us-can-help-prevent-them

Stern, Jessica and Berger, J. M. 2015. *ISIS the state of terror*. London: William Collins, 2015.

Sun Tzu and Griffith, Samuel. 2011. *The art of war*. 1st ed. London: Watkins Publishing, 2011.

Zald, Mayer and McCarthy, John. 1987. *Social movements in an organizational society.* New Brunswick, NJ: Transaction Books, 1987.

Wiktorowicz, Quintan. 2005. *Radical Islam Rising: Muslim extremism in the West.* Lanham, MD: Rowman & Littlefield Publishers, Inc., 2005.

If NATO deterrence fails, can the Baltics use unconventional warfare to overcome Russian occupation? MAJ Michael D. Hoffman

Introduction

In 2016, The Rand Corporation (a United States based think-tank) released an influential report on the results of a series of war-games conducted to determine possible outcomes of a Russian military offensive against the Baltic states (Estonia, Latvia, and Lithuania). In general, the results were heavily one-sided towards Russia. The three most significant outcomes of the study were (Shlapak, et al., 2016):

1) Without additional NATO defensive support, the longest it would take the Russian forces to reach the capitals of Latvia and Estonia was 60 hours.
2) To prevent an overrun of the Baltics, a sizable NATO ground force is required - 'seven brigades [3,000-5,000 personnel each], including three heavy armoured brigades—adequately supported by airpower, land-based fires' (Ibid).
3) If Russia succeeded in quickly seizing the Baltics, NATO would have three bleak options: a costly counteroffensive, direct escalation against Russia globally, or concession (at least temporarily) of the Baltics to Russia.

Under these circumstances, acknowledging the limits of NATO's deterrence and defensive capabilities[2], what can the Baltic states do to address the threat from a significantly larger and more capable military aggressor? Historically, this is not a unique problem. Since World War II, there has been at least 181 noteworthy examples of small armed forces fighting (both successfully and unsuccessfully) against stronger conventional militaries (Jones, 2017 p. 13). In these examples, the weaker forces utilized unconventional warfare (UW), defined as 'operations and activities that are conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area' (United States Joint Chiefs

[2] Since the publishing of the RAND report, NATO has amplified its deterrence effort through the Enhanced Forward Presence (eFP) initiative - four rotational battalion-size battlegroups (~ one brigade), which operate alongside their host countries' defence forces (Estonia, Latvia, Lithuania, and Poland) (North Atlantic Treay Organization, 2017). However, since these units are a fraction of the Rand study's recommendation, the author underlines eFP 'forces remain insufficient to prevent a rapid Russian [overrun of the Baltics]' (Shlapak, 2017).

of Staff, 2014). The ‘occupier’ versus ‘resistance movement’ scenario described in this definition is directly applicable to the conclusions of The Rand Corporation study.

If NATO deterrence fails, can the Baltic states use UW to overcome Russian occupation? This essay will argue UW is the Baltics’ best method to independently counter Russian occupation, and far more realistic than a conventional approach[3]. However, it requires a pragmatic and proactive effort, because there are many ways such a strategy could be ineffective or defeated outright. To argue how the Baltic states can be successful, the following essay will study the issue from three angles: lessons from past resistance movements in the Baltics, case studies of Soviet/Russian defeats to unconventional forces, and the advantages of embracing UW as a primary defensive strategy for the Baltics. While resistance movements typically contain multiple dimensions (governance, societal, etc.), this essay will focus primarily on the military component.

Chapter 1: The Legacy of the Forest Brothers

Estonia, Latvia, and Lithuania each engaged in armed resistance, or partisan warfare, against Soviet occupation after World War II. These resistance fighters, or ‘Forest Brothers’, remain a source of pride for the Baltic countries as a symbol of resistance and strength during a dark period of their history.

The defeat of the ‘Forest Brother’ movements contain many applicable lessons for a modern-day effort. While achieving some initial success and maintaining an active resistance from the mid-1940s to early 1950s, the Soviets eventually defeated each countries’ resistance movements due to a combination of factors. Understanding the causes of defeat provide valuable lessons, which a modern resistance strategy must understand and counter. In general, the ‘Forest Brothers’ were ill prepared for long-term resistance against a superior and ruthless occupation force. Specifically, two

[3] *Conventional warfare* refers to tactics and strategies used in direct combat between traditional militaries (e.g. land battles with infantry/armour/artillery or sea battles with warship fleets). It typically consists of large units with significant logistical requirements. *Unconventional warfare* avoids direct confrontation against a more powerful enemy through use of small units, mobility, surprise, and deception. The intention is not to defeat the enemy outright, but erode their morale and resolve. UW employs hit-and-run tactics like ambushes, sabotage, and raids, but can also include more controversial methods like assassinations and terrorism (Asprey , 2016).

Soviet tactics ultimately made it impossible for the resistance groups to survive without external support. The first tactic was infiltration of the groups by Soviet agents – both volunteers and forced collaborators. The second tactic was to cut off local support for the resistance groups through collectivization of farms and mass deportations (or ‘purges’), which eliminated access to resupply and shelter.

- Lithuanian - targeted purges (40,000 in 1948 and 29,000 in 1949) and collectivisation of farms destroyed the resistance’s support base and forced it underground (Gaskaite-Zemaitiene, 1999 p. 37). The Soviets eliminated the remaining members ‘mainly by using agents recruited from among the arrested partisans. The long underground struggle, difficult living conditions, the deportation of supporters […] had broken the will of some [arrested] partisans’ (Ibid, pp.42-43).
- Latvia - Faced similar Soviet tactics, including large purges of 280,000 people between 1943 and 1945 (Strods, 1999 p. 150). The Latvian resistance also struggled with organizational weaknesses including: few experienced leaders and difficulties forming a chain of command; a shortage of arms, uniforms, ammunition, and medical aid; and a lack of intelligence on the enemy’s tactics (including infiltration), numbers, and resolve (Ibid, pp.159-160).
- Estonian – Initially, the Estonians had some advantages. The Nazi’s abandoned large quantities of arms and ammunition as they retreated from Estonia, and many of the members were experienced veterans of the German army (Laar, 1999 pp. 214-219). However, Soviet intelligence, infiltration, and extensive use of mass deportation effectively nullified the movement’s impacts after the 1950s. The Soviets outlasted them - “every fallen KGB soldier was replaced by another, whereas the Forest Brothers had no resources to replenish their ranks” (Ibid, p. 228).

A modern resistance strategy should consider several lessons and warnings from this period. The ‘Forest Brothers’ suffered from a lack of preparation. While basic combat and guerrilla warfare skills are important, their downfall was due to lack of logistics, intelligence/counter-intelligence, command structure, and collective strategy. By proactively preparing a UW strategy in peacetime, the Baltic states can address and overcome these weaknesses. Specifically, a few anticipatory actions could be:

1. Establish command structures and teams to prevent the need to recruit new members (and potential hostile agents) later.

2. Establish and stockpile safe houses – provisions, ammo, weapons, and communications equipment.

3. Train intelligence and counterintelligence techniques to avoid detection and identify spies/collaborators.

4. Determine a collective resistance strategy designed around decentralized operations, including objectives and contingencies.

Overall, the intent is to minimize weak points for exploitation by the enemy, and create a clear plan now rather than improvise later. While any resistance movement requires societal support, proactive preparation can minimize this dependence, which will reduce risk to both the resistance movement and their supporters. UW victories do not come from defeating the enemy, but outlasting them.

Chapter 2: David Can Beat Goliath: Russian/Soviet Losses to Unconventional Forces

Beyond the Baltics, Soviet/Russian history of counter-insurgency (counter-UW) is notorious for 'enemy-centric' strategies. Rather than attempting to win over the population, it is characterized by brutal violence to supress any resistance (Ricks, 2009). In general, the Soviets/Russians have been remarkably successful at counter-insurgency. Russia has been victorious in almost 90% (18 out of 21) of its campaigns dating back to the early 1900s (Zhukov, 2011, p.12). For comparison, the global counter-insurgency success rate during the same period was 35% (Ibid). Since much of their successful operations were similar to their campaigns in the Baltics, the next section will focus instead on examining their losses. Specifically, Russian failures against irregular forces in Finland, Chechnya, and Afghanistan can expose potential weaknesses in the Russian approach.

Finland – During WWII, the USSR attempted to invade Finland with disastrous results. Finland's defence against the Soviets, also known as the 'Winter War', lasted 105 days (November 1939 to March 1940) and resulted in nearly 200,000 Russian casualties (1/3 of the invading army) (Rehman, 2016). The Fins succeeded by leveraging the harsh climate and employing an UW strategy. Significantly outgunned and outnumbered, the Finnish applied scorched earth tactics with an overall strategy of delay and progressive attrition of the enemy. They were experts at 'channelling, demoralizing, and diverting' the enemy (Ibid). Their tactics included mine warfare to force Soviet soldiers into ambushes; attacking lines of communication and supplies to worsen the already poor conditions; burning and/or extensively booby-trapping abandon territory and villages (Ibid). They targeted the enemy's ability to survive and made any conceded terrain dangerous and forbidding. While the Finnish lost border territory to the Soviets, 'Finland maintained its independence, and also gained the admiration of a world that saw a small, democratic nation standing up to an aggressive bully' (Peck, 2016).

Afghanistan – From 1979 to 1989, the Soviet Union fought a counter-insurgency war in Afghanistan in order to prop up the communist government. Anti-communist guerrillas (known as the Mujahedeen) fought the national government due to ruthless domestic purges and unpopular social welfare reform (Encyclopædia Britannica, 2018). The insurgents did not necessarily defeat the Soviet Army, but they outlasted them. After 10 years of little progress and mounting casualties, the Soviet Union withdrew due to loss of both military and domestic support.

The Mujahedeen were highly effective at the basics of guerrilla warfare. They avoided direct confrontation, emphasized surprise, employed terror, and took advantage of their knowledge of the terrain (Grau, 1996 p. 197). However, perhaps the most significant reason for their success was the Soviets' failure to isolate the Mujahedeen from outside support. The conflict served as a proxy war between the USSR and the USA, and as a result, the insurgents were exceptionally 'well equipped with US-supplied surface-to-air missiles, rockets, mortars, and communication equipment' (Reuveny, et al., 1999). The equipment support enabled the insurgents to inflict unacceptably high casualties and 'proved especially valuable in lessening the effectiveness of Soviet airpower and hitting Soviet morale' (Black, 2016 p. 185). The public outcry and opposition in the USSR surged as the dead and injured returned home (Reuveny, et al., 1999). The insurgent's ability to cause mass casualties at the tactical level ultimately led to strategic victory, but Russia's failure to isolate Afghanistan was the primary catalyst for this rare counter-insurgency failure (Blank, 2016 p. 81).

Chechen War I – Between 1994 and 1996, Russia lost a counter-insurgency war against separatists in the Chechnya region of Russia, even though the 'Russian

Federal forces enjoyed overwhelming superiority in all aspects of conventional war' (Janeczko, 2012). The Chechens succeeded tactically because they were highly effective at unconventional warfare fundamentals – ambushes, mines, improvised explosives, snipers, suicide bombers, and surface to air missiles (Meakins, 2017). Additionally, they were ruthless in applying psychological warfare – they 'created a climate of constant fear and ensured that Russian soldiers were in a permanent condition of stress and anxiety' (Ibid). These tactics included hanging Russian casualties from their defensive positions; booby-trapping dead bodies (both Russian and Chechen); use of snipers to injure rather than kill the enemy in order to lure and attack the rescue parties; and using Russian uniforms to enter bases for surprise attacks (Janeczko, 2012). The ultimate goal was to destroy the enemy's mind-set and morale, and they succeeded – 72% of Russian soldiers showed signs of psychological illness following the war (Ibid). However, the Chechens won the war not by affecting the morale of the military, but the Russian population. Because the theatre had few press restrictions, the Chechen rebels were able to broadcast their version of events, which resulted in sympathy for their cause (domestically and internationally) and 'widespread condemnation of the ineptitude and brutality of Russian forces' (Meakins, 2017). As in Afghanistan, it was not the casualties, but loss of domestic support, which caused Russia to withdraw.

<u>Lessons for the Baltics</u>: Each of these examples provides valuable insights, the Baltics should consider. The armed resistances in Finland, Chechnya, and Afghanistan were able to leverage their severe terrain/climate in ways the flat, temperate Baltics cannot. However, the descriptions above still provide applicable tactics/strategies. In general, the Baltic armed resistance must be prepared to be creative, resourceful, and most importantly ruthless. All three 'victories' only came after the unconventional forces inflicted enough casualties to decisively demoralize the enemy. Specific lessons from each are also important. Like the Finnish, the Baltics should focus on making their terrain inhospitable to the enemy. The lesson from Afghanistan is the importance of external lines of communication and support. Lastly, Chechnya provides a grim reality. Resistance forces must be prepared to terrorize the enemy, which requires them to suspend morality and any thought of 'fighting fair'. Both Afghanistan and Chechnya also demonstrate the importance of demoralizing not just the invading military, but also the domestic population.

Of note, Russia has also learned from these counter-insurgency failures. To avoid the heavy casualties, which lost them previous conflicts, the Russians have shifted to an over-reliance on indirect and aviation firepower in place of traditional land forces. In the second Chechen War (1999-2009), Russian extensive use of firepower greatly reduced insurgent asymmetric advantages (mobility), limited insurgent ability to inflict casualties (minimizing domestic unhappiness), and suppressed local support (Blank, 2016 pp. 86-87). Russia is currently using this same approach with 'devastating volume and intensity' in Eastern Ukraine (Wither, 2018). Additionally, Russia prioritizes isolating its theatre of operation, which includes information/media access as well as materiel support (Blank, 2016 p. 85). Baltic resistance forces should specifically guard against this strategy, because statistical studies have determined external support is the characteristic of insurgencies most strongly correlated with success (Jones, 2017 pp. 11-12; Johnston, et al., 2013 p. 8). Identifying these Russian adaptations does not invalidate the historical lessons above. If anything, it exposes that the Russians have also recognized these strategic vulnerabilities, which further supports the importance of exploiting them.

Chapter 3: An Unconventional National Defence Strategy

The Baltic states have recognized the threat of Russia quickly overrunning/overwhelming their conventional forces, as described in the introduction. As a result, all three countries have integrated UW (special operations, militia, and resistance forces) as elements of their national defence strategies (Estonian Ministry of Defence, 2011 p. 13; Latvian Ministry of Defence, 2016 pp. 7-9; Ministry of National Defence Republic of Lithuania , 2017 pp. 7, 14). These forces have undoubtedly considered many of the lessons identified in Chapter 1 and 2. However, despite the significant capability gap with Russia, conventional warfare remains the primary means of defence in these strategies. The third chapter will argue to maximize the capability of unconventional forces to resist Russian occupation, the Baltic states must recognize the futility of a conventional defence, and instead choose UW as the national defence strategy.

While potentially a provocative argument, two recent studies indicate this may become an increasingly mainstream recommendation for Baltic defence options against the

Russian conventional threat. In the first study, James Wither advocates for the Baltics to embrace an unconventional strategy for three primary reasons (Wither, 2018):

1. Emerging technologies (e.g. robotics, artificial intelligence and nanotechnology) will favour small, mobile, and self-sufficient teams over large, conventional forces. As a result, small states will be able to increasingly balance against more powerful adversaries, since conventional military capabilities will remain expensive and manpower intensive, and the costs for these emerging technologies will decrease over time.
2. Increasing spending on conventional capabilities may be politically important for fulfilling NATO obligations, but it 'diverts limited resources from territorial defence [UW] assets that arguably may prove more important in the event of a Russian invasion' (Ibid). The significant funding currently being spent on procuring and modernizing the Baltic states' conventional forces (Adamowski , 2017) would be far better invested in training and equipment (personnel carried anti-tank and anti-air weapons) for an unconventional defensive strategy.
3. A conventional focus distracts from important measures necessary to prepare for sustained UW including the acquisition, storage, and concealment of supply points, and training and preparations for urban guerrilla combat (the most likely terrain for modern UW).

The author of the second article, Karl Salum, also encourages small states facing a larger opponent to consider UW as a defence strategy, because they typically lack the resources, capabilities, and strategic depth to mount a conventional defence (Salum, 2018 p. 50). He identifies three options for integrating UW into a national defence strategy (Ibid). The first option is using UW as a covert back-up plan to a conventional defence. The second option is to fully integrate (and prioritize) UW in the strategy and actually use conventional forces to support UW efforts. The third option is to not only prioritize UW, but also advertise its capability to punish or deny the enemy as a method of deterrence.

Based on Wither's assessment (above), the Baltic states arguably fall mostly in the first option. Salum assesses there is a significant risk of failure in option one, because for UW to be an effective defensive strategy it requires at least equal authority and resources as the conventional forces for defensive preparations (Ibid). Additionally, a successful UW defence strategy requires a fundamentally different mind-set, which must be reflected in military doctrine, national law, government integration (whether standing, shadow, or exiled), external cooperation, and the understanding and support of the general population (Ibid pp. 65-66).

Both articles assert UW has realistic potential to defend against Russian occupation and aggression. Salum generally concludes ‘that UW is a feasible option for a small state defending against occupation’ (Salum, 2018 p. 48) and Wither’s conclusion explicitly states by employing UW across all phases of a defensive operation the Baltic states could deny, delay, and disrupt Russian attempts to occupy Baltic territory (Wither, 2018). However, the key principle underlying both articles is the necessity for the Baltic states to prioritize UW as their primary defensive strategy. To be successful, UW requires not just resources (advanced equipment, supply depth, and specific training), but also a significant change in mentality and institutional support.

Conclusion

The intention of the essay was to propose a solution to the problem identified by The Rand Corporation in the introduction. Against the Russian conventional threat, the Baltics must have an independent plan beyond NATO collective defence. This essay argues if NATO deterrence fails, the Baltic states could successfully employ unconventional warfare to resist a Russian invasion and occupation. However, to be successful, proactive and realistic preparations are required. Analysing the history of UW in the Baltics (the ‘Forest Brothers’) reinforces this point. Beyond being able to fight, this period proves an armed resistance must plan and prepare now to avoid the traps of improvising later. Prioritizing recruiting, logistics, supply depth, intelligence, and contingencies in peacetime are essential to outlasting the enemy in wartime. If these supporting efforts are in place, the case studies of Finland, Afghanistan, and Chechnya prove UW can defeat superior Russian conventional forces. These case studies also demonstrate UW forces must be innovative, resourceful, and ruthless in their attempts to simultaneously survive and wear down the occupation force. Lastly, it appears UW, as an official national defence strategy for small states, may soon become the preferred approach. With the right combination of advanced technology, specialized training, and domestic support (government and population), UW could not only be highly effective, but also far more practical than attempting to compete conventionally. In conclusion, the Baltic states can successfully resist Russian occupation with UW, but it requires learning from the past and taking action in the present.

Bibliography

Adamowski , Jaroslaw . 2017. Fear factor: As Russia looms large, Baltics up military capacity. *Defense News.* [Online] August 28, 2017. [Cited: April 03, 2018.] https://www.defensenews.com/smr/european-balance-of-power/2017/08/28/fear-factor-as-russia-looms-large-baltics-up-military-capacity/.

Asprey , Robert Brown. 2016. Guerrilla Warfare: Military Tactics. *Encyclopædia Britannica.* [Online] Encyclopædia Britannica, Inc., July 14, 2016. [Cited: April 3, 2018.] https://www.britannica.com/topic/guerrilla-warfare .

Black, Jeremy. 2016. *Insurgency and Counterinsurgency: A Global History.* Lanham, MD : Rowman and Littlefield, 2016.

Blank, Stephen. 2016. Russian Counterinsurgency in Perspective. [ed.] Beatrice Heuser and Eitan Shamir. *Insurgencies and Counterinsurgencies: National Styles and Strategic Cultures.* Cambridge : Cambridge University Press, 2016.

Encyclopædia Britannica. 2018. Soviet invasion of Afghanistan. *Britannica Online Encyclopædia .* [Online] 01 05, 2018. [Cited: 01 20, 2018.] https://www.britannica.com/event/Soviet-invasion-of-Afghanistan.

Estonian Ministry of Defence. 2011. *National Defence Strategy Estonia.* 2011.

Gaskaite-Zemaitiene, Nijole. 1999. The Partisan War in Lithuania from 1944 to 1953. *The Anti-Soviet Resistance in the Baltics.* Vilnius : Genocide and Resistance Research Centre of Lithuania, 1999.

Grau, Lester W, [ed.]. 1996. *The Bear Went Over the Mountain: Soviet Combat Tactics in Afghanistan.* Washington, D.C. : National Defense University Press, 1996.

Janeczko, Matthew N. 2012. The Russian Counterinsurgency Operation in Chechnya Part 1: Winning the Battle, Losing the War, 1994 – 1996 . *Small Wars Journal.* 2012.

Johnston, Patrick B and Jones, Seth G. 2013. The Future of Insurgency. *Studies in Conflict & Terrorism.* 2013, Vol. 36, pp. 1-25.

Jones, Seth G. 2017. *Waging Insurgent Warfare: Lessons from the Vietcong to the Islamic State.* New York : Oxford University Press, 2017.

Laar, Mart. 1999. The Armed Resistance Movement in Estonia from 1944 to 1956. *The Anti-Soviet Resistance in the Baltic States.* Vilnius : Genocide and Resistance Research Centre of Lithuania, 1999.

Latvian Ministry of Defence. 2016. *The National Defence Concept (Latvia).* Riga, Latvia : s.n., 2016.

Meakins, Joss. 2017. The Other Side of the Coin: The Russians in Chechnya. *Small Wars Journal.* [Online] January 15, 2017. [Cited: April 5, 2018.] http://smallwarsjournal.com/jrnl/art/the-other-side-of-the-coin-the-russians-in-chechnya.

Ministry of National Defence of the Republic of Lithuania. 2017. *National Security Strategy.* Vilnius, Lithuania : s.n., 2017.

North Atlantic Treay Organization. 2017. Boosting NATO's presence in the East and Southeast. *North Atlantic Treay Organization.* [Online] Decemeber 21, 2017. [Cited: January 05, 2018.] https://www.nato.int/cps/en/natohq/topics_136388.htm.

Osburg, Jan. 2016. *Unconventional Options for the Defense of the Baltic States: The Swiss Approach.* Santa Monica : RAND Corporation, 2016.

Peck, Michael. 2016. How Finland Lost World War II to the Soviets, But Won Peace. *The National Interest.* [Online] August 19, 2016. [Cited: April 01, 2018.] http://nationalinterest.org/feature/how-finland-lost-world-war-ii-the-soviets-won-peace.

Rehman, Iskander. 2016. Lessons from the Winter War: Frozen Grit and Finland's Fabian Defense. *War on the Rocks.* [Online] 07 16, 2016. [Cited: 10 18, 2017.] warontherocks.com /2016/07/lessons-from-the-winter-war-frozen-grit-and-finlands-fabian-defense/.

Reuveny, Rafel and Prakash, Aseem. 1999. The Afghanistan war and the breakdown of. *Review of International Studies.* 1999, 25.

Ricks, Thomas E. 2009. Counterinsurgency: The brutal but effective Russian approach. *Foreign Policy.* [Online] September 17, 2009. [Cited: April 01, 2018.] http://foreignpolicy.com/2009/09/17/counterinsurgency-the-brutal-but-effective-russian-approach/#.

Salum, Karl. 2018. Small State UW Doctrine: Feasibility and Application for National Defense. [ed.] Kevin D Stringer and Glennis F Napier. *Resistance Views: Essays on Unconventional Warfare and Small State Resistance.* MacDill Air Force Base, Florida : Joint Special Operations University Press, 2018.

Shlapak, David A and Johnson, Michael W. 2016. *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics.* Santa Monica : Rand Corporation, 2016.

Shlapak, David. 2017. Deterring Russian Aggression in the Baltic: What It Takes to Win. s.l. : Committee on Armed Services Subcommittee on Tactical Air and Land Forces United States House of Representatives, 01 March, 2017.

Strods, Heinrihs. 1999. The Latvian Partisan War between 1944 and 1956. *The Anti-Soviet Resistance in the Baltic States.* Vilnius : Genocide and Resistance Research Centre of Lithuania, 1999.

Zhukov, Yuri M. 2011. Counterinsurgency in a Non-Democratic State: the Russian Example. [ed.] Paul Rich and Isabelle Duyvesteyn. *The Routledge Handbook to Insurgency and Counter Insurgency.* London : Routledge, 2011.

United States Joint Chiefs of Staff. 2014. *Joint Publication 3-05: Special Operations.* Suffolk, VA : United States Department of Defense, 2014.

Wither, James K. 2018. "Modern Guerrillas" and the Defense of the Baltic States. *Small Wars Journal.* 2018.

Is social network theory the most suitable for understanding terrorist radicalisation within Europe? MAJ Sean Navin

Introduction

Since 2001, Islamic terrorist organisations and lone wolves have conducted attacks in Belgium, France, Germany, the United Kingdom, Spain, and other countries, bringing the wars of the Middle East to the streets of European cities. Spotlighting terrorism, media coverage has placed growing attention towards Islamic extremist groups. Such attention has consequences. Extremist groups can no longer operate in the physical domain without unwanted monitoring from Western governments. As a result, their tactic has shifted to inspiring lone wolves, those who self-radicalise and execute acts of violence in the name of Islamism. This essay will draw examples from the Islamic State in Iraq and Syria (ISIS) and its influence on the process of radicalisation within social networks and lone wolves.

The benefit of understanding radicalisation is that it allows for the development of strategy. It focuses on identifying the source of radicalisation, in order to counter and disrupt the radicalisation process.

The United States' Federal Bureau of Investigation defines radicalisation as 'the process by which individuals come to believe their engagement in or facilitation of non-state violence to achieve social and political change is necessary and justified' (Hunter, 2011). The process of radicalisation can occur in a group setting, as well as within an individual. With lone wolf attacks currently on the rise, the problematic issue is determining which path of radicalisation offers the more valuable analysis. Solving this issue would enable the development of a counter radicalisation strategy. This essay will argue that although lone wolves demonstrate radicalisation, their individual breakdown falls short of the understanding offered through the analysis of social network theory, which provides more insight into European terrorist radicalisation by the study of existing relationships and connectivity.

Though many factors exist, this essay outlines the radicalisation process in three stages: first, the motivation or the why, second, the recruitment or the how, and third, violent action or the what. This outline will shape the structure of the arguments presented in this essay. Before discussing the process of radicalisation, a description of social network theory and self-radicalisation will be provided.

In regards to the process, the first aspect of radicalisation is motivation, ranging from personal ambitions, dissatisfaction with current affairs, fear, revenge, and/or religious beliefs. Both social networks and lone wolves can share similarities in motivation. The manipulation of motivation allows for the potential of recruitment.

The second aspect is recruitment, and it will be argued that radical Islamic groups recruit members into their organisation through physical interactions and the virtual community. The radicalisation of a lone wolf lacks the use of physical recruitment methods. After recruitment, one embraces a radical ideology that often leads to the commitment of violence.

Finally, in the most critical part of indoctrination into radical terrorist groups, followers are encouraged to conduct violent acts. These attacks achieve their desired results: incitement of terror, reaction of governments, and further promotion of radical Islamic organisations. An analysis of these attacks prove the completion of the radicalisation process. Prior to the conclusion, case studies will be provided to further illustrate why social network theory is more suitable than self-radicalisation.

Paths to Radicalisation

It is important to understand the physical make up of each path of radicalisation, in order to visualise the flow of ideology within the radicalisation process. A social network starts at the centre, a hub, where all ideology and beliefs originate. The information reaches smaller groups, or nodes, through common connection, otherwise known as links (Sageman, 2004 p. 137). In the case of Islamic radicalisation, the initial common connection is often religiously based. Mosques and social communities present themselves as attractive nodes for further expansion. Within these nodes are smaller groups, or cliques, which create strong connections via friendship or familial ties (Sageman, 2004 p. 152). The flow of information travels between associated nodes. The interconnectivity and possibility of new connections to the hub allow for the exponential growth of the radical message.

An alternative to radicalisation within a group is self-radicalisation. Lone wolf actors are individuals, or up to two to three people, with minimal to no support from a network

(Simon, 2013 p. 266). Able to operate undetected, lone wolves perform as an army of one, with no direction or objectives from a central headquarters. Lacking obvious connections to the larger network, the lone wolf is responsible for his or her own radicalisation.

Motivation behind Radicalisation

The initial stage of the radicalisation process requires motivation. The presence of multiple factors within a social network and its members acts as the compelling force towards radicalisation. These factors stem from personal necessity, but evolve into achieving an objective for the greater good of a collective organisation. Uncovering core motivations is greatly possible through the study of social network theory. Research shows those who join extremist organisations desire belonging to a community, offering unity and a sense of purpose. A common sense of purpose and duty binds ISIS fighters together (Penman, et al., 2015). Some members of extremist organisations are not deep believers in extremist doctrine (Borum, 2012 p. 9), but the feeling of community and a need of protecting those who share common values are powerful influencers. Marc Sageman, former CIA officer, argues that Muslims participate in jihad because of common norms, values, and worldviews (Sageman, 2004 p. 143).

By joining an extremist group, members gain a cultural identity, where before he or she may have felt ostracised from Western society. Peter Neumann, founder of the International Centre for the Study of Radicalisation and Political Violence, conducted research showing 20% of foreign fighters within ISIS originated from Western European countries (Neumann, 2016 p. 72). Discrimination against alienated European Muslims is a key motivator for members of these social networks to join radical terrorist organisations. Threatening feelings from outside sources can force a person or group to look inwards towards familiarity (Al Raffie, 2013 p. 73). Jocelyne Cesari, research associate at Harvard’s Centre for European Studies, offers that radicalisation in Europe occurs as a social process because of four contributing elements: the presence of radical ideology, discrimination and alienation of Muslims, disregarded subdivision of European youth, and lack of nationalism (Cesari, 2011 p. 103). This disassociated community lives by an Islamic way of life, values, and beliefs of their own design. With proprietary feelings over this culture, it is a natural progression to protect and defend it against outside threats. People are willing to kill in defence of their friends, families, and culture (Sageman, 2004 p. 156). Understanding how motivation propels one towards recruitment offers valuable data, illustrating the shift from individual thought to the adoption of group mentality. This analysis is crucial to creating a strategy to counter further stages of radicalisation.

While mirroring similar motivations to those of a social network, lone wolves seek radicalisation for more personal, selfish objectives. Due to the internal nature of the lone wolf, it is difficult to pinpoint a core motivation behind self-radicalisation. Though they often sympathise with cultural or political ideology, lone wolves act alone. Lacking the requirement to pledge loyalty, the lone wolf can maintain a personal agenda in shaping their mission (Simon, 2013 p. 41). In 2003, Jessica Stern, research professor of global studies, conducted a study highlighting the motivation of the combination of personal grievances and ideology in the self-radicalised terrorist (Teich, 2013 p. 5). Brian Jenkins, senior advisor at the RAND Corporation, categorises the most vulnerable population as those looking for approval, identification and validation (Jenkins, 2007 p. 3). Prior to becoming a lone wolf, individuals may have tried to join an extremist group, but were deemed too volatile and ultimately denied membership (Simon, 2013 p. 42). Feeling socially alienated contributes to the development of an isolationist attitude (Pantucci, et al., 2015 p. 9). With this rejection, one may choose the path of self-radicalisation, in order to prove their solitary act is just as effective. Unbounded by the constraints of a specific network, lone wolves provide their own source of identity and power to achieve hero status, opinions obtained from the outside world.

The lone wolf, by definition, has individual motivations unique to each person. Studies of multiple lone wolf actors would provide little pattern in their path to radicalisation when compared side by side. However, within a social network, a person possesses individual thoughts, but due to the pressure of the community, acts in accordance with the group mentality, thus providing a core motivation. Research into social network theory provides a formulation of patterns based on relationships and connection to others. A social network's motivations are evident, therefore useful in the analysis of the radicalisation process.

Recruitment towards Radicalisation

The second stage of the radicalisation process is the routes by which one undergoes recruitment. Thomas Olesen, scholar of social movement theory, describes these routes to recruitment as an organisation seeking out an individual, a person seeking out an organisation, or recruitment through family and friends (Olesen, 2009 p. 8).

As an example of an organisation seeking out members, ISIS issues a call to jihad by disseminating propaganda championing their cause in fighting the injustices of the world (Penman, et al., 2015). Compelled by motivations, individuals seek out organisations, such as ISIS, as evidenced by European Muslims joining the jihad during the Bosnian war (Neumann, 2016 p. 47). Current members of terrorist groups recruit family and friends to join their organisations. Marc Sageman's 2004 study of 172 jihadists discovered approximately 75% joined as a group or had pre-existing social ties to current members (Bakker, 2011 p. 134). Once recruited into an organisation, the individual mind transforms towards the group mentality. Studies on social movement theory show that individuals will adopt the mentality of the group thinking and change their behaviour to match that of the group (Al Raffie, 2013 p. 77). The collective thinking of the group acts as a catalyst during the recruitment process, inciting fellow members of networks to adhere to the direction of the network. Peer pressure within networks strengthen the commitment of the individual to join the cause (Dalgaard-Nielsen, 2008 p. 8). It can be argued that an analysis of recruitment methods within a group provides a two-way road map between the organisation and the individual. This study provides quantifiable demographics that often share a link to other recruits via previous connections.

The process of radicalisation of the lone wolf actor is the sole responsibility of the individual, and as a result, the routes of recruitment are applied differently. The internet provides extremist groups a platform to spread radical beliefs and ideology through a multitude of sources. A twenty-four hour business, it allows open access to upload and download information. Never before has it been easier to find both radical material and instruction for violence (Pantucci, et al., 2015 p. 3). The internet provides a forum for information but is contingent on individuals seeking out the information. The self-radicalised person seeks out extremist ideology, harnesses the teachings, and ultimately internalises the message of others into their own belief system. In 2007, Brian Jenkins said ‘self-radicalisation begins the day that an individual seeks out jihadist websites’ (Jenkins, 2007 p. 3). With a few strokes of the key, an individual can establish one-way contact with a multitude of extremist sites. This gave rise to a number of spokespersons, to include Anwar Al-Awalki, the so-called ‘god father of lone wolf terrorists’ (Simon, 2013 p. 139). Al-Awalki gave video sermons, often having no physical contact with those he radicalised, yet was successful due to the virtual world. Individuals also engage in online forums with like-minded believers. Within these virtual communities, members further recruitment by sharing ideas and inciting one another into action. The internet plays a vital role in the formation of loosely connected groups, whose members are of like-minded thinking (Koomen, et al., 2016 p. 183). This allows the lone wolf to connect to others, yet maintain a sense of isolation and anonymity. An analysis of the lone wolf recruitment phase is only visible through the virtual world. Without internet monitoring, it would be nearly impossible to gain insight into the self-radicalised recruitment process.

Recruitment is a requirement in both social network theory and self-radicalisation. Through the three routes of recruitment, social networks benefit from both physical interactions and virtual connections. This provides a visible network analysis of an organisation, highlighting the linkage across multiple groups. Both paths are aided by the use of an online community, which indicates a connection between individuals and organisations. Websites are not enough; connection reinforces radicalisation. It could be argued that there is no true lone wolf, but are in fact, subsets of an overall social network. Gabriel Weimann, professor of communication, concluded the lone wolf ‘may operate alone, but they are recruited, radicalised, taught, trained, and directed by others’ (Weimann, 2012 p. 79). Unless a lone wolf communicates to the outside world, it is nearly impossible to discover the recruitment process self-imposed upon the individual. However, the recruitment process within a social network can be examined through the study of relationships and connectivity.

Commitment to Radicalisation

The final stage in the process of radicalisation is the commitment of violence in the name of extremist ideology. Terrorist attacks on innocent lives are the most concrete evidence of the radicalisation process and the dangers it represents to society. Both groups and individuals commit attacks, yet lone wolves denote a smaller fraction of overall terrorist attacks. In a study conducted by Ramon Spaaij, senior research fellow, sampling fifteen countries on terrorist activity between 1968 and 2010, only 1.8% of over 11,000 incidents were carried out by lone wolves (Simon, 2013 p. 240). This statistic illustrates the larger sample size of network terrorist attacks available for analysis. In analysing attacks conducted by networks, the existence of multiple actors allows for the exposure of links between actors, the group, and the overall terrorist network. These links can trace the process of radicalisation, to include the motivation, methods of recruitment, and the core source of radical ideology and beliefs. Each violent act committed by a lone wolf is unique, providing no linkage to another lone wolf's violent act. What makes one individual kill is not the same for another. Furthermore, it is difficult to establish their motivation and means of recruitment, due to gaps in connectivity within the process. In using social network theory, one can visualise the complete radicalisation process from beginning to end, or trace from point of violence to original source of radicalisation. Social network theory highlights linked groups of individuals, whose radicalisation process potentially affords the revelation of pattern and commonality. These patterns can be used in developing counter-radicalisation strategies, in an attempt to interrupt or circumvent the radicalisation process.

Case Studies

Case studies offer the opportunity to analyse the radicalisation process. An example of social network theory, highlighting the effect of networks on radicalisation in Europe, is the Salafi movement. This study shows insight into the importance of connections and relationships. Due to the discontent of Western influence over Muslim countries and values, the Salafi movement was born. The desire was to return to pure Islam based off Sharia law, with this intent still practiced today (Neumann, 2016 p. 36). Salafi communities are present in most major European cities. They provide a safe environment for Muslims to meet, exchange ideas, and interact with other members (Sageman, 2004 p. 143). Neumann's research found that jihadists, foreign fighters originating from Europe, were associated with Salafi mosques prior to membership of terrorist organisations (Neumann, 2016 p. 112). This study is worth notating, because it is an example of how terrorist organisations manipulate a pre-existing group with common motivation and recruit members into a radical group, who then execute violent acts. Analysis shows the Salafi community as a prime pool of potential recruits for terrorist organisations. ISIS uses the connectivity of Salafi members throughout Europe to their advantage. By using social network theory, researches can trace members and their paths to radicalisation because of common factors such as shared relationships and motivations. This provides a clear depiction of who, why, and how one becomes radicalised, allowing a counter-strategy to focus on the root causes of radicalisation within this group.

The purpose of the following two case studies is to demonstrate the individuality and incomparable nature of lone wolf attacks. They choose targets, plan, and execute attacks all of their own design. Two recent examples of lone wolf terrorism, the Bastille Day and Berlin Christmas market attacks in 2016, detail violent acts, without providing an understanding into the individual's radicalisation process. Mohamed Lahouaiej-Bouhlel conducted a solo attack by driving a truck into a Bastille Day celebration in Nice, France, killing 87 people and wounding 433 (Global Terrorism Database, 2017). ISIS claimed responsibility after the attack. Upon investigation, authorities discovered ISIS propaganda on his computer, yet he was unknown to have ties with the organisation (Counter Extremism Project, 2018). Lahouaiej-Bouhlel had a record of petty crime and domestic abuse. Considered not to be a religious individual, two weeks prior to the attack, he downloaded radical material from the internet (Counter Extremism Project, 2018).

Later that year, Anis Amri, Tunisian born, drove a truck into a crowded market, killing 12 and wounding 48 people (Global Terrorism Database, 2017). Prior to his attack, ISIS released a video of Amri pledging allegiance. After years of petty crime and imprisonment, he sought asylum in Germany under false documentation. Amri was denied citizenship, and over the next year proceeded to download Islamic extremism content and reach out to radical Salafi imams (Counter Extremism Project, 2018). An investigation revealed Amri used encrypted social media to share his plans with like-minded individuals (Counter Extremism Project, 2018).

It can be argued that analysing lone wolf attacks provide little pattern and connectivity into the overall radicalisation process. Looking at these lone wolf cases, an analysis can only suggest what motivated each one to self-radicalise. In both cases, one is left without a clear understanding as to the why and how behind their radicalisation process, therefore making it difficult to construct a counter-strategy.

Conclusion

In response to radicalised Islamic organisations and their terrorist attacks, Western Governments have embarked on a mission coined the War on Terror. However, this phrase suggests an end or victory over terrorism, presumably achieved using military force. This is unlikely. History shows if you remove one terrorist, ten quickly rise to the cause. To truly influence change, it is necessary to comprehend the process of radicalisation.

By understanding the process, there is potential to discover ways to disrupt or even prevent further radicalisation. For this reason, it is more suitable to use social network theory to understand radicalisation. One can gain knowledge of motivating factors, methods of recruitment, and operational strategy in conducting attacks. Yet in the case of lone wolves, their process is left more to speculation than fact. In addition, lone wolves are a collection of outliers lacking a link to each other, prohibiting analysis outside the individual. As previously discussed, the study of social networks provides quantifiable data into the process of radicalisation, with an emphasis on the importance of relationships and connections. In solidifying understanding radicalisation through social network theory, Joel Busher, research fellow, said 'study after study has pointed to the importance of social networks for processes of socialisation into radical social or political action' (Busher, 2015 p. 1). In order to develop a counter-radicalisation strategy, there must exist a solid appreciation for the understanding of the radicalisation process. Relationships and connectivity within a radicalised group allow for pattern analysis into the overall radicalisation process, where one is able to trace each stage of radicalisation down to its core source. Because of social network theory, one can gain an education into the physical make-up, motivations, and methods of recruitment within the radicalisation process. Only through this knowledge can a counter-radicalisation strategy be created and effective.

Bibliography

Al Raffie, Dina. 2013. Social Identity Theory for Investigating Islamic Extremism in the Diaspora. *Journal of Strategic Security Volume 6.* [Online] 2013. [Cited: March 6, 2018.]

https://pdfs.semanticscholar.org/e85a/45123bbc73b199a4443b29c0e36ede079442.pdf.

Bakker, Edwin. 2011. Characteristics of Jihadi Terrorists in Europe (2001-2009). [book auth.] Rik Coolsaet. *Jihadi Terrorism and the Radicalisation Challenge.* Surrey : Ashgate, 2011.

Borum, Randy. 2012. Radicalisation into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security 4, no. 4, 7-36.* [Online] 2012. [Cited: September 27, 2017.] http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1139&context=jss.

Busher, Joel. 2015. What Part Do Social Networks Play in Radicalisation? *Radicalisation Research.* [Online] Radicalisation Research, July 6, 2015. [Cited: September 25, 2017.] http://www.radicalisationresearch.org/debate/busher-social-networks/.

Cesari, Jocelyne. 2011. Muslims in Europe and the US: A Shared but Overrated Risk of Radicalism. [book auth.] Rik Coolsaet. *Jihadi Terrorism and the Radicalisation Challenge.* Surrey : Ashgate, 2011.

Counter Extremism Project. 2018. *Counter Extremism Project.* [Online] 2018. [Cited: March 21, 2018.] https://www.counterextremism.com/extremists/mohamed-lahouaiej-bouhlel.

Counter Extremism Project. 2018. Counter Extremism Project. [Online] 2018. [Cited: March 21, 2018.] https://www.counterextremism.com/extremists/anis-amri.

Dalgaard-Nielsen, Anja. 2008. Studying Violent Radicalisation in Europe I: The Potential Contribution of Social Movement Theory. *Danish Institute for International Studies.* [Online] 2008. [Cited: March 6, 2018.] http://pure.diis.dk/ws/files/56375/WP08_2_Studying_Violent_Radicalisation_in_Europe_I_The_Potential_Contribution_of_Social_Movement_Theory.pdf.

Global Terrorism Database. 2017. Global Terrorism Database. [Online] University of Maryland, 2017. [Cited: December 15, 2017.] https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201612190002.

Global Terrorism Database. 2017. Global Terrorism Database. [Online] University of Maryland, 2017. [Cited: December 15, 2017.] https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201607140001 .

Hunter, Ryan. 2011. Radicalisation of Islamist Terrorists in the Western World. *Law Enforcement Bulletin.* [Online] Federal Bureau of Investigation , September 1, 2011. [Cited: March 27, 2018.] https://leb.fbi.gov/articles/perspective/perspective-radicalisation-of-islamist-terrorists-in-the-western-world.

Jenkins, Brian Michael. 2007. Building an Army of Believers: Jihadist Radicalisation and Recruitment. *RAND Corporation.* [Online] April 5, 2007. [Cited: September 26, 2017.] https://www.rand.org/content/dam/rand/pubs/testimonies/2007/RAND_CT278-1.pdf.

Koomen, Willem and Van Der Pligt, Joop. 2016. *The Psychology of Radicalisation and Terrorism.* New York : Routledge, 2016.

Neumann, Peter R. 2016. *Radicalised: New Jihadists and the Threat to the West.* London : I.B. Tauris & Co. Ltd, 2016.

Olesen, Thomas. 2009. Social Movement Theory and Radical Islamic Activism. *Centre for Studies in Islamism and Radicalisation.* [Online] May 2009. [Cited: March 6, 2018.] http://www.ps.au.dk/fileadmin/site_files/filer_statskundskab/subsites/cir/pdf-filer/H%C3%A6fte2final.pdf.

Pantucci, Raffaello, Ellis, Clare and Chaplais, Lorien. 2015. Lone-Actor Terrorism Literature Review. *Royal United Services Institute for Defence and Security Studies.* [Online] December 2015. [Cited: March 19, 2018.] https://www.isdglobal.org/wp-content/uploads/2016/02/Literature_Review.pdf.

Penman, Maggie and Vedantam, Shankar. 2015. The Psychology of Radicalisation: How Terrorist Groups Attrack Young Followers. *NPR.* [Online] NPR, December 15, 2015. [Cited: October 2, 2017.]

http://www.npr.org/2015/12/15/459697926/the-psychology-of-radicalisation-how-terrorist-groups-attract-young-followers.

Sageman, Marc. 2004. *Understanding Terror Networks.* Philadelphia : University of Pennsylvania Press, 2004.

Simon, Jeffrey D. 2013. *Lone Wolf Terrorism Understanding the Growing Threat.* Amherst : Prometheus Books, 2013.

Teich, Sarah. 2013. Trends and Developments in Lone Wolf Terrorism in the Western World: An Analysis of Terrorist Attacks and Attempted Attacks by Islamic Extremists. [Online] October 2013. [Cited: December 19, 2017.] https://i-hls.com/wp-content/uploads/2013/11/Lone-Wolf-Sarah-Teich-2013.pdf.

Weimann, Gabriel. 2012. Lone Wolves in Cyberspace. *Journal of Terrorism Research.* [Online] September 22, 2012. [Cited: March 19, 2018.] https://cvir.st-andrews.ac.uk/article/10.15664/jtr.405/.

BEST ESSAY OF THE CIVIL SERVANTS COURSE (CSC)

What are the future prospects of the eFP in the Baltic region? Mr. Marko Brügel

‘Deploying US units to Estonia would be like showing a red flag to the bull’.[4] (Laaneots, 2014)

Introduction

While Russia’s actions in annexing Crimea in 2014, continued support to rebels in eastern Ukraine, and bellicose rhetoric have shocked the foundations of the post-Cold war geopolitical stability in Europe and brought risk of open conflict to a considerable probability, NATO’s reaction in reassuring its eastern flank members and adapting to a more deterrent posture has been timely, visible and credible. On top of the reassurance measures adopted in 2014, including the establishment of six new NATO Force Integration Units, increased air-policing assets, naval group patrols on the Baltic Sea, and a Very High Readiness Joint Task Force (VJTF), the 2016 Warsaw Summit added new elements in NATO’s deterrence and defence posture - the formation and deployment of four multinational enhanced Forward Presence (eFP) battlegroups in each of the three Baltic countries and Poland, as well as plans to develop tailored forward presence in the Alliance’s Black Sea region. In short, the Alliance is currently sending a strong message of deterrence.

However, NATO’s forward deployed eFP battlegroups can only be a means to an end in deterring Russia’s foreign policy ambitions, so their future size, duration, and ultimately *raison d’etre* is subject to competing external threat perceptions and internal conflicts within NATO. It follows that in the post medium-term, mission fatigue and abundance of other external or internal problems will likely cause Allies to lose political appetite for long-term eFP contributions in the Baltics. Therefore, parallel measures in the Baltic region must be developed, which will serve as NATO’s deterrence baseline after eFP’s withdrawal. These measures should include reinforcement, staging and

[4] General Laaneots (Estonian Chief of Defence 2006-2011) commenting on a remark made by Defence Minister Urmas Reinsalu that the last US tank withdrawn from Europe should have been deployed to Estonia for permanent presence. The comment comes five and a half years after the 2008 Georgia-Russia war.

prepositioning capabilities, regular high-visibility exercises, and the continuous development of host nations' own forces.

This essay attempts to analyse the role played by currently deployed eFP battlegroups in NATO's defence and deterrence posture, what spoilers within the Alliance could crack the foundation of this newfound cohesion, and offers suggestions for maintaining a baseline credible deterrence, should lowered threat perceptions result in the withdrawal of the eFP.

The 'New Normal' – eFP as game changer in NATO's adaption

Although the security environment on NATO's eastern flank took a turn for the worse by the mid-2014, the concerted decision to deploy actual Allied troops did not come in haste, and it was only in July 2016 that NATO's Secretary General Jens Stoltenberg announced at the Warsaw summit that:

> '... we have decided to enhance our military presence in the eastern part of the Alliance. With four battalions here in Poland, as well as Estonia, Latvia and Lithuania on a rotational basis. These battalions will be robust and multinational. They demonstrate the strength of the transatlantic bond. And they make clear that an attack on one Ally would be considered an attack on the whole Alliance'. (Stoltenberg, 2016(a))

Indeed, as Allers points out the West's initial reaction to Russia's aggressive actions concentrated on a combination of sanctions and diplomacy, with emphasis on refraining from conflict escalation and violating the NATO-Russia Founding Act. However, the new focus on deterrence by presence was a decisive step forward from the assurance measures adopted the Wales summit two years earlier, and sent a clear signal that NATO would respond as one to any aggression (Allers, 2017 p. 24-26).

This cohesion of the Alliance is accentuated by the multinationality of the battlegroups, as the current and pledged eFP contingents include eighteen different NATO nations under four framework nations in each of the host nations (NATO, 2017). Of special note are the considerations of the framework nations, as in addition to the USA's persistent presence in the region since 2014, the UK affirms in a post-Brexit world that 'with the largest defence budget in Europe … and our position at the heart of NATO, the UK's role in Europe's defence has never been more vital' (The Independent, 2017), that Canada leading NATO deterrence efforts is a core mission in its new Defence Policy (Sajjan, 2017), and that Germany is emerging from its traditional non-military role, despite Chancellor Merkel rejecting the possibility of stationing troops in Latvia, Lithuania and Estonia on a long-term basis two years prior to the Warsaw summit (Deutsche Welle, 2014).

However, a thornier issue of the eFP is its *credibility* of deterrence. As Luik and Praks have pointed out, 'an essential element of the credibility of the deterrent is the perception of military capability to inflict substantial costs on an attacker and deny it an ability to quickly achieve its objectives' (Luik and Praks, 2017 p. 8). While the battlegroups include heavy armour and are declared combat-ready, RAND think tank war gaming scenarios on Baltic defence have concluded that a sufficient Allied force against estimated Russian capabilities would entail about seven brigades, including three heavy brigades – with adequate support from air, land-based fires, and various enablers on the ground (Shlapak and Johnson, 2016). Notwithstanding the mismatch, NATO's current presence can be considered to represent a 'strong symbol of NATO's deterrent tripwire' (Marten, 2017 p. 27), where Baltic and Polish national forces are supported by the deployed eFP troops (among them three nuclear powers and United Nations Security Council permanent members), and the recently established rapid reaction units of NATO's Very High Readiness Joint Task Force.

Future prospects of the eFP in the Baltic region

As earlier mentioned, the forward deployed eFP battlegroups can only be a means to an end in NATO's deterrence toolbox, so their future size and duration is subject to competing external threat perceptions and internal conflicts within NATO. To put it another way and borrowing from constructivist theorist Alexander Wendt's idea that 'anarchy is what states make of it' (Wendt, 1992), then also the eFP is what NATO makes of it. A fixed state of animosity or goodwill between the West and Russia is not set as a law of physics, and therefore pending future developments, the eFP's current dimensions can grow to larger and permanent forces, or be eventually withdrawn.

Based on the prevailing security climate in which Russia's aggressive rhetoric and annexation of Crimea continues, the conflict in eastern Ukraine looks destined for a frozen conflict, and Vladimir Putin's most probable re-election for president of the Russian Federation will establish a similar course for the next six years, there is little evidence for a shrinkage in the security dilemma or an overhaul of relations initiated by either side to improve the situation (Timofeev 2016 p. 63-64). Indeed, according to DSACEUR Everard, NATO's own planned next steps will be to strengthen the eFP with air force and naval elements, which 'will allow for the further improvement of the deterrence and defence capabilities of the battle groups stationed in the region' (ERR, 2017). Countering arguments of these being escalatory steps by NATO, Kulesa and Frear conclude that 'Russia has no objective grounds for seeing the forces which are being currently forward deployed as a move aimed as escalating tensions. There seems to be space to add further elements … while remaining in line with the general tenets of NATO's modern deterrence and the NATO-Russia Founding Act' (Kulesa and Frear, 2017 p. 6).

However, there are elements that could sway the balance in NATO's threat perception scale in the medium to long term. Firstly, as a blessing or curse, since eFP deployments as a mission have no clearly defined political end state nor 'mission accomplished' parameters, their continuation in contribution pledges ranges from indefinite to whenever political appetite dictates it. While it is understood that all NATO decisions are taken *at 29* consensus basis, if Russia's bilateral diplomatic efforts to fragment the Alliance (on issues such as trade, energy supply or fighting ISIS) bear fruit, this consensus on continuing the same level of deterrence could decrease. This currently unlikely scenario would be further plausible in case of 'Russia fatigue' among the Allies, or settling for a bargain that returns Ukraine its eastern regions. After all, president Obama's reset with Russia was initiated only 8 months after the Georgia-Russia war (BBC News, 2009).

Secondly, as Praks remarks, as 'the global security environment remains volatile and its development unpredictable' (Praks, 2017 p. 31), the focus on regional security in the Baltic area can be affected by other international or national events that influence decision-makers in NATO or EU countries. These may include the flare-up of the confrontation with North Korea, turmoil in NATO's southern flank, need for more troops for national causes in case of increase in domestic terror attacks following the return of radicalized fighters from the Middle East, or change in national leadership.

In short, precluding drastic changes in the current security climate, it is more than probable that eFP battlegroups or their enhanced versions will be anchored to the

Baltic region in the short to medium term. However, medium to long term presence is subject to internal or external factors that shape policymaking in the Alliance's capitals.

Enablers for maintaining deterrence in the long term

As presented above, the current tenets of NATO's deterrence and defence posture on its eastern flank, as manifested through the deployment of eFP, subscribe to former NATO SACEUR General Breedlove's warning that 'virtual presence means actual absence' (Breedlove, 2015 p. 9). On the other hand, simply based on geography, Russia has the constant strategic advantage of keeping permanent actual presence in its Western military district with a much lower cost-to-effect ratio.

However looking ahead, and factoring in a possible de-escalation in the current NATO-Russia standoff, it is worth examining NATO's *modern* deterrence as envisioned by Secretary General Stoltenberg. This construct would not rely on Cold War style matching the opponent in numbers, but would include a combination of forward presence, 'supported by a programme of exercises… with the right infrastructure and prepositioning of equipment to facilitate rapid reinforcement' (Stoltenberg, 2016(b)). The latter part of these elements could form the future baseline of deterrence, if actual forward presence contributions become unpalatable for the Allies. Similar sentiment was echoed at NATO's high-level 'Evolving Modern Deterrence Posture' workshop in May 2017. As Kulesa and Frear summarize, 'NATO must address significant challenges in resuscitating the military science of reinforcement, follow-on forces and infrastructure, both physical and organisational. [...] This aspect of NATO's modern deterrence must be well-resourced and exercised'. (Kulesa and Frear, 2017 p. 4). Additionally, relevant stakeholders have expressed requests for freedom of movement of NATO forces, including guaranteed access to rail lines and heavy transport, improved intra-theatre mobility regulations, and expanding staging and marshalling capacities (Conference, 2017).

Work to address these capability gaps has already commenced, as evidenced by calls for a military Schengen zone in Europe (Politico, 2017) and NATO's common funded infrastructure projects to support pre-positioning, receiving and supporting reinforcement of troops, and expansion of training areas (NATO, 2016; DOD, 2016 p. 6). This infrastructure can upon completion, together with a regular Baltic region focused exercise regime, be a conduit for the visibility of NATO's Very High Readiness Joint Task Force.

Underlying all these measures will be the continued effort of all Allies to contribute to fulfilling the Defence Investment Pledge – 2% of GDP on defence, of which 20% shall be allocated to major procurements – agreed upon at the 2014 Wales Summit, and the continuous development of national forces and capabilities. This applies especially to the current eFP battlegroups' host nations, as it would be a signal to other Allies that host nations are not merely security consumers, but also security providers.

Conclusions

Following Russia's resurgent geopolitical aggressiveness, NATO's reaction in reassuring its eastern flank members and adapting to a more deterrent posture has been timely, visible and credible. However, the forward deployed eFP battlegroups can only be a means to an end in deterring Russia's foreign policy ambitions, so their future size, duration, and ultimately *raison d'etre* is subject to competing external threat perceptions and internal conflicts within NATO.

Precluding drastic changes in the current security climate, it is more than probable that eFP battlegroups or their enhanced versions will be anchored to the Baltic region in the short to medium term. However, medium to long term eFP presence is subject to internal or external factors that shape policymaking in the Alliance's capitals. While noting that virtual presence is actual absence, NATO's new *modern* deterrence also underscores, in parallel to forward deployed forces, capabilities for rapid reinforcement, visible exercises, and right infrastructure for prepositioning and staging. Backed up by adequate defence resources and continued development of host nations' forces, the listed capabilities could form NATO's Baltic region deterrence baseline after eFP's possible, or eventual withdrawal.

Bibliography

Allers, Robin. 2017. Modern Deterrence? NATO's Enhanced Forward Presence on the Eastern Flank. *NATO and Collective Defense in the 21st Century. An Assessment of the Warsaw Summit.* 2017.

BBC News. 2009. Pressing the US-Russia reset button. *BBC News*. [Online] 5 March 2009. [Cited: 31 October 2017] http://news.bbc.co.uk/2/hi/americas/7926096.stm

Breedlove, Philip M. 2015. United States European Command Theater Strategy. *US EUCOM*. [Online] October 2015. https://www.eucom.mil/media-library/document/35147/useucom-theater-strategy

Conference. 2017. BALTDEFCOL Conference, held under Chatham House rules. Tartu, Estonia. 2017.

Deutsche Welle. 2014. Latvia asks Merkel for greater NATO presence in Baltic. *Deutsche Welle*. [Online] 18 August 2014. [Cited: 31 October 2017] http://www.dw.com/en/latvia-asks-merkel-for-greater-nato-presence-in-baltic/a-17861456

DOD. 2016. DOD Military Construction Program FY 2017 Budget. *US Department of Defense*. [Online] February 2016. [Cited: 31 October 2017] http://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2017/budget_justification/pdfs/11_NATO_Security_Investment_Program/FY2017_NATO_Security_Investment_Program.pdf

ERR. 2017. NATO to strengthen Baltic region defense with air, naval forces. *ERR News*. [Online] 20 September 2017. [Cited: 31 October 2017] http://news.err.ee/619668/nato-to-strengthen-baltic-region-defense-with-air-naval-forces

Kulesa, Łukasz; Frear, Thomas. 2017. NATO's Evolving Modern Deterrence Posture: Challenges and Risks. *ELN Issue Brief: Deterrence*. [Online] May 2017. [Cited: 31 October 2017]
http://www.europeanleadershipnetwork.org/medialibrary/2017/05/18/de5cc379/NATOs%20Evolving%20Deterrence%20Posture%20-%20ELN.pdf

Laaneots, Ants. 2014., Laaneots: USA üksuste toomine Eestisse oleks kui punane rätik pullile (Laaneots: deploying US units to Estonia would be like showing a red flag to the bull). *Postimees*, [Online] 8 January 2014. [Cited: 31 October 2017] https://www.postimees.ee/2655022/laaneots-usa-uksuste-toomine-eestisse-oleks-kui-punane-ratik-pullile

Luik, Jüri; Praks, Henrik. 2017. Boosting the Deterrent Effect of Allied Enhanced Forward Presence. *ICDS Policy Paper*. [Online] May 2017. [Cited: 31 October 2017] https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Policy_Paper_Boosting_the_Deterrent_Effect_of_Allied_eFP.pdf

Marten, Kimberly. 2017. Reducing Tensions Between Russia and NATO. *Council of Foreign Relations, Council Special Report No. 79*. [Online] March 2017. [Cited: 31 October 2017] https://www.cfr.org/sites/default/files/pdf/2017/03/CSR_79_Marten_RussiaNATO.pdf

NATO. 2016. Warsaw Summit Communiqué (paragraph 37d). *NATO homepage*. [Online] 9 July 2009. [Cited: 31 October 2017] https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. 2017. Boosting NATO's presence in the east and southeast. *NATO homepage.* [Online] 11 August 2017. [Cited: 31 October 2017] https://www.nato.int/cps/en/natohq/topics_136388.htm

Politico, 2017. Call for 'military Schengen' to get troops moving. *Politico*. [Online] 9 August 2016. [Cited: 31 October 2017] https://www.politico.eu/article/call-for-military-border-schengen-to-get-troops-moving-nato-eu-defense-ministers/

Praks, Henrik. 2017. Estonia and the Military Aspects of the Security of the Baltic Sea Region. *Security in the Baltic Sea Region: Realities and Prospects*. 2017.

Sajjan, Harjit S. 2017. Canadian-led NATO Battlegroup begins work in Latvia. *Government of Canada homepage*. [Online] 19 June 2017. [Cited: 31 October 2017] https://www.canada.ca/en/department-national-defence/news/2017/06/canadian-led_natobattlegroupbeginsworkinlatvia.html

Shlapak, David; Johnson, Michael.2016. Reinforcing Deterrence on NATO's Eastern Flank. *RAND Corporation*. [Online] 2016. [Cited: 31 October 2017] https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1253/RAND_RR1253.pdf

Stoltenberg, Jens. 2016(a). Press conference on 8 July 2016 by NATO Secretary General Jens Stoltenberg following the meetings of the North Atlantic Council at the level of Heads of State and Government. *NATO homepage.* [Online] 9 July 2016. [Cited: 31 October 2017] https://www.nato.int/cps/en/natohq/opinions_133276.htm

Stoltenberg, Jens. 2016(b). Speech by NATO Secretary General Jens Stoltenberg at the Munich Security Conference. *NATO homepage.* [Online] 15 February 2016. [Cited: 31 October 2017] https://www.nato.int/cps/en/natohq/opinions_128047.htm

The Independent. 2017. Theresa May to claim Britain's role in Europe's defence 'has never been more vital'. *The Independent*. [Online] 28 September 2017. [Cited: 31 October 2017]
http://www.independent.co.uk/news/uk/politics/theresa-may-brexit-security-eu-estonia-visit-defence-a7972891.html

Timofeev, Ivan. 2016. Russia and NATO in the Baltic. *The Baltic Sea Region: Hard and Soft Security Reconsidered.* [Online] 2016. [Cited: 31 October 2017] http://liia.lv/en/publications/the-baltic-sea-region-hard-and-soft-security-reconsidered-558

Wendt, Alexander. 1992. Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization*, Vol. 46, No. 2 (Spring, 1992), pp. 391-425.

How can Latvia enhance its societal resilience to better counter Russian propaganda? Mr. Roberts Saulītis

‘A society’s ability to defend itself crucially depends on its population having a critical mind.’ (Jan Joel Anderson, 2015)

Over the last few years Russia’s comprehensive and contemporary way of war in Eastern Ukraine and Crimea has initiated widespread debates among international and national policy-makers, academics, media and public on the overall nature of so called “hybrid warfare” or “hybrid threats” and possible tools to counter them. Although there are no agreements about definition of “hybrid warfare” concept, one of the central elements for mobilising own population and demonising adversaries is information. Russia’s Chief of the General Staff, General Valery Gerasimov, in his article in 2013 commented that for Russia information is seen as a species of weapon and a mean of great power (Gerasimov, 2013, p. 24). Therefore state-sponsored and coordinated Russian propaganda with the aim to shape public opinion, promote Russian values and discredit the West, has become the main tool of non-military threat to coherence of societies in Baltic states. In this complex situation where Latvia is countering internal and external threats posed by Russia experts have been advocating for national security policy which includes enhancement of societal resilience. This concept is described as the ability of nation-state, society or community to preserve its cohesion and to cope with external and internal stresses caused by socio-political, environmental and/or violent disturbances (Bambals, 2016, p. 48; Jermalavičius 2015, p. 160).This paper argues that despite the fact that societal resilience is a hard to measure long-term government strategy with uncertain effects, the enhancement of societal resilience in Latvia is decisive to counter Russian propaganda by creating pluralistic information environment, developing government organised strategies, raising awareness about threats and increasing trust in government institutions.

To answer the essay question this paper will look at the aim of Russian propaganda and applied methods to achieve it; examine the characteristics of societal resilience, its relationship with deterrence and impact in Latvian society; and suggest implementation of various measures to counter external and internal threats by enhancing societal resilience in Latvia.

The tools and aim of Russian Information Warfare in Latvia

The existence of linguistically divided information space in nowadays Latvia provides a platform for Russian speaking media to influence Latvian society, especially a large part of Russian-speaking community. By using broad spectrum of tools, Russian propaganda aims to influence public opinion by arguing that Latvia suppresses Russian minorities, that Latvia is a "failed state" and has become a puppet to Western powers.

Before addressing how, why and on what topics Russian propaganda has ability to influence Latvian society it must be understood what concept of propaganda includes and what tools are used to achieve its aim. H. Kula defines propaganda as 'the process of influencing people, shaping their attitudes and internalizing behaviours aimed at the accomplishment of political goals' (Kuczynka-Zonik, 2016, p. 44). Disinformation and propaganda, both centrepieces of hybrid warfare, have become an effective tool accompanying military operations to exercise the influence of society, challenge its stability and resilience. The aim of Russian propaganda is to confuse truth with fiction, promote and defend Russian culture, ideology and values, justify Kremlin's decisions by disparaging Western values and political authorities (Meister, 2016, p. 1).

Russian government is using a broad spectrum of methods and tools to spread propaganda in Latvia, for example, state-financed media (RT, PBK, Sputnik) and other media outlets (Vesti, RuBaltic, Baltnews), government organized NGOs (Russkij Mir and Rossotrudnichestvo), social media (Youtube, twitter, Facebook), professional internet "trolls", "opinion agents" or pseudo-intellectuals (Vladimirs Lindermans, Aleksandrs Gapoņenko and Josifs Korens) (Latvian Security Police, 2017, p. 12-18). Media research conducted by research company "TNS" supports the claim, that previously mentioned agents have a broad platform to influence Latvian society. In the first half of 2017 Russian TV channel "PBK" was the third most watched channel in Latvia (8.1%) and all of the channels in Russian language made up 30.0% of overall TV audience (TNS, 2017). In printed media Russian newspaper "MK Latvija" for the last two years has been the most read newspaper (audience - 330 000) according to the average audience of one edition (TNS, 2016). Various propaganda examples are spread through media, for example that "The ruling coalition of Latvia is "raping" Russians" (Tarasov, 2017), that "Latvia is dying out. There is nobody to work" (Pushkarev, 2017) or that "Latvia has asked USA to occupy it" (Baltijalv, 2015).

Not all of the evidence supports argument that a linguistically divided information space in Latvia exists and it poses significant threat to national security. Firstly, broadcasts of Latvian Television covers 99% of Latvia's territory. Although in border area, signals from Russian on Belarussian broadcasters are stronger, official state news are reachable for all citizens. Secondly, by analysing statistics it's visible that besides two propaganda "flagships" – PBK and "MK Latvija" other actors are unable to attract large audience. Latvian Security Police has concluded that influence of Russian propaganda agents is decreasing, because Russia has limited financial resources to support them and it causes internal disputes between individuals and organisations (Latvian Security Police, 2017, p. 16-17). Despite these disputes the existence of Russian disinformation and propaganda tools poses a significant challenge to national security, integrity and societal coherence in Latvia. Existence of Russian media connects its audience to Russian world-view, decreases diaspora's need to learn the official language and weakens their integration (Kuczynka-Zonik, 2016, p. 54).

Societal resilience as a counter measure to Russian propaganda

Ability for Russian propaganda to reach large part of Latvian society, linguistically divided information space and the slow pace on minority integration has revealed vulnerabilities between social groups in Latvia. One of the possible solutions to integrate and stabilize the society against threats is to enhance societal resilience.

By using F. Norris model societal resilience is dependent on four inter-related resources – economic development, social capital, community competence and information and communication (Jermalavičius, 2015, p. 160-161). Resilience's main focus lays on societal security, ability to overcome adversities, shared knowledge and skills which are exercised through social interactions (Bambals, 2016, p. 51-52). In

Latvia's case enhancement of societal resilience helps to narrow channels through which propaganda is being exercised. Building society's capacity to anticipate, evaluate and solve challenges can contribute to deterrence by reducing attackers' potential gains. This essay will concentrate of community competence that refers to society's collective efficacy and information and communication dimension 'which include trusted sources of accurate information (…) and collective narratives' (Jermalavičius, 2015, p. 161). Before making the first steps to enhance societal resilience, it is important to identify vulnerable groups or regions that are more exposed to external and internal tensions (Jaitner, 2015, p. 93).

The most vulnerable societal group to external hybrid threats including information warfare in Latvia is Russian-speaking minority. It should be emphasized, that Russian-speaking community doesn't pose risks by themselves, but the risk lays in possible manipulation with it. Comprehensive Russian propaganda "machine" which includes "Compatriot's policy", ideological tools like culture, educational system and language policy, victimization of Russian-speaking minority, divided information space and slow pace of minority integration has revealed deep gaps and different understandings between social groups about external threats to state's security (Reire, 2016, p. 10). In a situation where public sees Russia as an aggressor and possible threat to Baltic States sovereignty, Russian-speaking community sees it as the only choice to orient Latvia's foreign policy to and the best associate for Baltic region (Reire, 2016, p. 10-11).

Multiple problems emerge when analysing the impact of societal resilience to counter Russian propaganda. First, resilience is a broad concept that encompasses full spectrum of elements and social scientists haven't developed indicators to measure it. Second, resilience can't be seen as the only option to counter propaganda. The Ukrainian crisis shows that before the deployment of conventional forces, Russia used different methods in all sectors to destabilize situation in border regions. Third, official statistics shows that integration process of Russian-speaking minority is accelerating and level of welfare has risen, narrowing gaps that could lead to possible vulnerabilities. (Zvirbulis, 2017) To conclude, societal resilience can be helpful to fight information warfare and deter further Russian ambitions to influence Latvian society only when combined with necessary political, economic and diplomatic measures taken and government should implement determined measures to enhance societal resilience.

Suggestions for enhancing societal resilience in Latvia

Enhancement of societal resilience in Latvia asks for a comprehensive approach from government institutions, NGO's, media and public to counter Russian information warfare. Possible measures for enhancing societal resilience in Latvia to counter Russian propaganda can be divided in long-term and short-term offensive and defensive measures. Offensive includes targeting the source of propaganda, but defensive are aimed at building society's ability to cope with external and internal stresses.

Adoption of clear and relevant legal framework needs to be the primary defensive long-term measure for enhancing resilience. It needs to include the definition of hybrid warfare elements, what threats they pose to national security and what tool it implements for all state actors to counter the threats. For Latvia, the first steps were taken in 2016, when amendments in Criminal Law aimed at actions carried out against Republic of Latvia and assistance to other states in same manner were passed (Latvijas Vēstnesis, 2016). Other measure for official state media to reach whole Latvian society should include creating a multi-language approach. Latvian public broadcasting system should introduce state-sponsored media outlets in Russian language to create pluralistic information environment. This can be seen as both a short-term and a long-term strategy, because diversity of Russian-speaking media and introduction of common liberal Western values to Russian-speaking community should work as an alternative to Russian propaganda and unfold half-truths and misleading information. Another important aspect to enhance societal resilience of Russian-speaking minority is for government to close the gap between state's policy and public needs and perception. Political environment in Latvia after the restoration of independence has been divided by ethnicity. By implementing "us-them" strategy, political parties for the purpose of gaining votes have fragmented Latvian society. Increasing civic participation and trust for both – governmental and national organisations – is a vital tool to integrate Russian-speaking community in political processes.

Another important element for enhancing societal resilience in a long-term would be a strong public education system. Latvia should unify education system only in Latvian language and promote courses for high school student's that develop critical thinking – history, political science (with orientation to international relations) and philosophy. For general public national government should develop a public diplomacy program to raise awareness about information manipulation, disinformation, falsification and provide basic civil defence and crisis management training to address potential security risks (Bambals, 2016, p. 71). Such programs have proved their usefulness in Finland where education system combined with comprehensive government strategy has been one of the reasons for society's high resilience to Russian information warfare (Standish, 2017).

Not all of the academics and politicians agree that only defensive measures need to be implemented to fight Russian propaganda, although offensive measures have to be target-oriented and closely coordinated not to oppose freedom of speech, Western democratic principles and polarize relationship with Russian community. Latvian officials should strengthen the capacity of The National Electronic Mass Media Council (NEPLP) to implement and broaden legislature for restriction of propaganda agents (broadcasters, journalists and websites) if information in their programs is tendentious, falsifies history or implements hate speech. For example, Latvian officials should take Lithuanian example and suspend broadcasting of Russian TV channels ("PBK", "RTR Planeta", et.al.). Lithuanian regulatory agency has suspended broadcasting several times in a past few years of a period of 3 to 6 months (European Commission, 2017). Although the range of offensive measures is not wide, the right defensive and offensive measures for each case needs to be implemented to successfully enhance societal resilience and counter Russian propaganda.

Conclusion

This essay argues that in the last couple of years Russia has intensified its information warfare against Latvia, focusing on Russian-speaking minority. Its aim is to manipulate with society by influencing public opinion and confusing truth with fiction. Using broad set of methods and platform offered by Russian-speaking media in Latvia, propaganda has an ability to reach its audience. One possible way for Latvian officials to preserve cohesion of society and counter Russian propaganda against external and internal threat is by enhancing societal resilience. By using F. Norris theoretical framework essay argues that societal resilience can help to narrow channels through which propaganda is being exercised.

How can Latvia enhance societal resilience to counter Russian propaganda? It can be done by implementing comprehensive defensive and offensive measures. These include adoption of relevant legislature, strengthening public education system by unifying it only in Latvian language and strengthening capacity of NEPLP to implement restrictions of propaganda agents. National government should develop public diplomacy program to raise awareness about misinformation and intensify fight against corruption, as it can help to increase trust of government institutions.

Enhancement of societal resilience is an essential tool to overcome societal vulnerabilities and can serve as an ingredient of deterrence, but it can't be seen as the only antidote to counter hybrid threat which is posed by Russian information warfare.

Bibliography

Bambals, Rihards. 2016. Societal Resilience: The Case of the Russian-speaking Community in Latvia. Žaneta Ozoliņa, ed. *Societal Security: Inclusion-Exclusion Dilemma. A portrait of the Russian-speaking community in Latvia*. Riga : Zinātne, 2016.

European Commission. The decision to suspend broadcast of the Russian language channel "RTR Planeta" in Lithuania complies with EU rules. [Online] 2017. [Cited: 10 October 2017] https://ec.europa.eu/digital-single-market/en/news/decision-suspend-broadcast-russian-language-channel-rtr-planeta-lithuania-complies-eu-rules.

Gerasimov, Valery. 2016. The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Military Review, 2016.

Jaitner, Margarita. 2015. Russian Information Warfare: Lessons from Ukraine. Kenneth Geers, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn : NATO CCD COE Publications, 2015.

Jermalavičius, Tomas. 2015. Societal Resilience as a Deterrent in 'Hybrid War'. Andris Sprūds, Kārlis Bukovskis, ed. *Towards Reassurance and Solidarity in the Euro-Atantic Community*. Riga : Latvian Institute of International Affairs, 2015.

Krimināllikuma grozījumi: sods par valsts pamatinterešu apdraudējumu. 2017. [LV portal, Amendments to Criminal Law: punishment for threats to national interests] [online] 2017. [Cited: 4 October 2017] http://m.lvportals.lv/visi/skaidrojumi?id=278939.

Kuczynka-Zonik, Aleksandra. 2016. Russian propaganda: methods of influence in the Baltic States. *Yearbook of the Institute of Eastern-Central Europe*, 2016, Vol. 14, 2.

Латвия вымирает. Работать некому, 2017. [Pushkarev, Timur, 2017. Latvia is dying out. There is nobody to work] [Online] 2017. [Cited: 12 October 2017] http://vesti.lv/news/kadrovyi-golodomor-pribaltika-otkryvaet-dveri-dlya-gastarbaiterov/print.

Латвия просит США оккупировать её, 2015. [Baltijalv, 2015. Latvia has asked USA to occupy it] [Online] 2015. [Cited: 9 October 2017] http://baltijalv.lv/news/read/25892.

Latvian Security Police. 2016. gada publiskais pārskats. 2017. [Latvian Security Police, Public Report of 2016] [online] 2017. [Cited: 7 October 2017] http://dp.gov.lv/lv/noderigi/gada-parskati/.

Mazākumtautību pārstāvju piederības sajūta Latvijai stiprinās, 2017. [Zvirbulis, Ģirts, 2017. The sense of belonging to Latvia strengthens for minority representatives. Latvijas Avīze] [Online] 2017. [Cited: 11 October 2017] http://www.la.lv/piederibas-sajuta-stiprinas/.

Meister, Stefan. 2016. *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign*. Washington : Transatlantic Academy, 2016.

Nacionālā preses auditorijas pētījuma rezultāti 2017. gada pavasarī. 2017. [TNS, Results of the National Press Survey in spring 2017] [online] 2017. [Cited: 2 October 2017] http://www.tns.lv/?lang=lv&fullarticle=true&category=showuid&id=5133&mark=telev%C4%ABzija.

Reire, Gunda. 2016. *Resilience of the Baltic Countries against Russia's Foreign Policy. Executive Summary*. Rīga : Zinātne.

Standish, Reid. 2017. Why is Finland Able to Fend off Putin's Information War? *Foreign Policy*. [online] 1 March 2017. [Cited: 8 October 2017] http://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/

Правящая коалиция Латвии «насилует» русских, 2017. [Tarasov, Anatolii, 2017. The ruling coalition of Latvia is "raping" Russians] [Online] 2017. [Cited: 12 October 2017] http://vesti.lv/news/pravyashtaya-koaliciya-latvii-nasiluet-russkih.

TNS. 2016. gada konsolidētās TV skatītākais kanāls-TV3. 2016. [TNS, 2016. Consolidated TV Most Popular Channel in 2016-TV3] [online] 2016. [Cited: 2 October 2017] http://www.tns.lv/?lang=lv&fullarticle=true&category=showuid&id=5094&mark=Konsolid%C4%93t%C4%81s|TV|skat%C4%ABt%C4%81kais|kan%C4%81ls.

BEST ESSAY OF THE HIGHER COMMAND STUDIES COURSE (HCSC)

What kind of impact will emerging technologies have on the armed forces over the next 10 years? LTC Aleksander Andric

Introduction

'*Beam me, Scotty*!' is a folk saying from the series Star Trek, which could be echoing in reality over a millennium. Authors of science fiction were always good at predicting the future - from the flight to the moon to the uprising of artificial intelligence (Bratič, 2018).

Scientifically fiction stories like *Twenty Thousand Leagues Under the Sea* and later stories of traveling to space and battles there, unbeatable robots and the superpower of new weapons originating from high-tech technology, as well as today's heroes using lasers and supersonic weapons have always been attracted by people of all ages, regardless of whether they have been presented in books, cinemas, DVDs or other media. Today, we often find them in various professional magazines and articles, as well as in defence documents and are no longer a fantasy, they become a reality. The resentment of the super-techno weapon, however, has a bearing on the community and its impact on the reason, time and place and the way of the development of the war.

Over the last two decades, information technology has expanded to almost all activities and to most work areas, including the armed forces. Different types of digital, semi-automated and automated processes are present almost everywhere, both in the work environment and in everyday private activities. Our activities of the mind and the body, the activities of the entire society are increasingly connected with various technologies, and some experts and futurologists say that we are entering a transhuman or post-human phase of existence, which is characterized by an increasing interconnection with technology. 'Professor Klaus Schwab, chairman and founder of the World Economic Forum, argues that the collapse of barriers between digital and physical, and between synthetic and organic, constitutes a Fourth industrial revolution, promising a level change comparable to that brought about by steam power, electricity and computing' (Schwab, 2016).

The development of military technology has become a big deal with the emergence of big and small development companies and research agencies, in addition to traditional military defence development institutions. ‘They created what President Dwight Eisenhower called in his farewell address a “military-industrial complex”, a perpetual arms race, not necessarily with any particular enemy, but with the status quo’ (Roland, 2009).

This essay will confirm that emerging technologies will have an impact on the armed forces over the next ten years. Given the wide range of emerging technologies and the analysis of their impact on modern warfare, this essay will argue that, even though technology development will have a significant impact on the armed forces, it will not replace the human element in conflicts. The human is a key player who decides if he will or will not go into an armed conflict and how he will lead it. Technology only offers him the opportunity to help achieve his goals with more sovereignty and fewer casualties. The technologies and their potential military use in the next ten years will be presented and their impact analysed. Military strategic planners are already deeply engaged in these technologies, as they need to define the place and the mission very accurately and integrate the technologies into the structure. That changes the wholesome structure of the armed forces and the strategy and tactics of warfare. In addition, the essay will investigate what these technologies can mean for the future and whether all new technologies are actually also practical and versatile.

The essay consists of five chapters. The introductory part presents the topic, defines the subject, purpose and the structure of the essay. The second part presents the scientific and technological progress with regard to the armed forces, the importance of it, its indicators and what are the overall trends in the development of the armed forces, especially in developed countries. The third part presents the implication of these trends in the armed forces. The advantages and disadvantages of progress and the fact that human remains the main factor in spite of the technology are presented in the fourth part. The latter part outlines the facts that support the claim that the development of technologies will affect the armed forces over the next ten years, but that the person remains in the first place.

Scientific-technological development and its implications on the armed forces

According to the professor (lecture delivered under the Chatham House rule):

> The use of new technologies for military purposes has two objectives: improving the capacity of its own forces compared to the forces of opponents in situations similar to battles (operational advantage) and archiving strategic advantage with the ability to influence the full potential of the opponent (Notes, 2018).

So far, research and development in the field of military technology have emerged from the empirical fact that the lifetime of the average modern weapon system is about 15 years. 'Since the development of an armaments system takes from 6 to 8 years, followed by 1 to 3 years of testing, it is very important that we anticipate what the opponent will develop or construct in the next 6 to 8 years' (Žabkar, 1994). If developers are able to truly develop a technology that will upgrade, develop and update automatically, this cycle will drastically change to an unpredictable dimension. Detection, development, the use of advanced knowledge, the latest sciences and technology are essential to preserving the technological standard. 'The NATO Science and Technology Council (STO), with about 5000 scientists, engineers and analysts, has identified a list of twelve technological areas expected to have the largest impact on capabilities and operations in the future' (NATO STO, 2017).

SHOR-TERM *(<6 YEARS)*	*MID-TERM* *(6-20 YEARS)*	*LONG-TERM* *(>20 YEARS)*
1. Additive Manufacturing 2. Everywhere Computing 3. Predictive Analytics 4. Social Media 5. Unmanned Air Vehicles	6. Advanced Materials 7. Mixed Reality 8. Sensors are Everywhere	9. Artificial intelligence 10.Electromagnetic Dominance 11. Hypersonic Vehicles 12. Soldier Systems

Innovation in some of the most advanced areas of science and technology according to the Margaret Kosal:

> [ ] include robotics and autonomous unmanned system; artificial intelligence; biotechnology, including synthetic and systems biology; the cognitive neurosciences; nanotechnology, including stealth meta-materials; additive manufacturing (aka 3D printing); and the intersection of each with information and computing technologies, i.e., cyber-everything (2016).

On the other hand, 'that such technologies could yield doomsday scenarios and that military applications of such technologies have even greater potential than nuclear weapons to radically change the balance of power' and these concepts and their fundamental strategic importance were defined at the multinational level in the NATO Strategic Concept of May 2010 (Kosal, 2016). By developing the perception and understanding of potential threats, anticipating technological changes and predicting possible upcoming technologies military organizations such as 'NATO can take advantage and an opportunity to make better choices today about the required capabilities in the future' (NATO RTO, 2011).

Technological improvements affect the reliability of operation in particular, due to the automation of communication means, combat assets, control over the work of power units and control of the damage caused. In so far as automation also includes the infallibility and the possibility of constant adaptation to changes and their integration into the digitized command control network. New technologies emerge on a global level, they become cheaper and more accessible, communication with them and between them is faster every day, and various product manufacturers appear in different designs. The right to ownership of new technology has gone into oblivion. Çalişkan is convinced that it is becoming increasingly more important to possess new technologies than knowing them properly and use them appropriately and that when developing these technologies we must constantly search for answers to the question: 'What is the best way or method of using the new technology' (Çalişkan, 2017).

Artificial Intelligence

The term 'Artificial Intelligence (AI)' is understood as the ability of devices to equate themselves with people in terms of learning, inference, design, and performance in complex cybernetic physical environments. This practically means that AI is a substitute for human thinking, decision-making and control in all areas. 'AI is located in autonomous robots or vehicles, boats, aircraft, it carries out functions of automatic detection of information and detection of anomalies and their elimination, psychological operations and intelligent mentoring for various military and support missions' (Notes, 2018). By developing AI software they will be able to make faster decisions based on a much larger amount of data collected than human beings could. How far could the development of artificial intelligence go? 'By 2050, the computer power of 1000 USD will be equal to the processing power of all the brain on earth' (Evans, 2010). Also considering the possibility of 'smart dust' that will connect everything to the internet, which will allow us to monitor and manage our environment.

It's a fact that technology innovations are happening at a fast pace and the exponential growth of computational power, data storage, bandwidth, and the information is unthinkable. Computers will have self-aware abilities and no longer just exponentially cognitive abilities, because of this ability to instantly interpret things it will overcome language barriers.

AI is useful in all areas and has long since exceeded the capacity of man. It is capable of controlling weapons, including nuclear weapons. It can also be used to control everything and everyone, wherever a fast and current response is needed even before something happens – much faster than a human response. Brimley argues that ‘the success of future forces will depend on their ability to search, correct, and complete goals faster than their opponents’ (Brimley, 2018). At this speed, this led to further development and even faster AI performance, which means the faster collection, analysis and reaction. Everyone is aware that in the next war the winner will be the one who is faster, which is why everyone is striving for a faster and more sophisticated AI technology. The question is, is this development of technology under control and what does it bring? The superpowers are competing which one will develop an AI system that will be much better (faster) than the opponents. Can Russia take lead in developing AI and move the scale of weapons technologies and military domination on its side? ‘The statement of the Russian President, Vladimir Putin, who suggested that with the help of the AI, Russia could shift the power, speaks of how important, strong and influential is the AI. The state-sponsored media reported that AI “is of key importance for Russia” (Meyer, 2017). The Arms Control Arrangement is one of the mechanisms that were put in place to control arming, but at the moment there is no agreement on the AI to be included in this group, so it is currently not under control. As each AI can be used for military purposes it would be necessary, not only for official and regular armed forces, but also to prevent access to it for terrorist and other militant groups and organizations, non-state actors and individuals, as it allows for the creation of a massive destroying, threatens stability and allows for more possibilities of hybrid wars, which in turn means that conflicts are escalating to unpredictable consequences. There is also an ethical concern about AI technology. Did we come up with the idea of building AI, which will decide instead of us to cause harm to us, decide on a war and peace, on being or not being? State institutions create and prescribe legal and moral norms and also control. Will AI systems, if they are able to make a decision, be responsible for their consequences? However, ‘there are fears that with the use of a variety of AI applications such as drones, self-driving vehicles and cybersecurity, we may again enter into another cold war’ (Straub, 2018). As we are in the constant anticipation of some of the major change and the use of new technologies and their appropriate tactics, the units have constantly increased the state of alert, which on a longer period leads of doubt and uncertainty.

Robotics

Robotics can be defined as a science fiction from the recent past that became a reality. A robot is defined as a ‘machine with sensors, processors, and effectors able to perceive the environment, have situational awareness, make appropriate decisions and act upon the environment’ (Echevarria II, 2009). They are characterized by being devastating, surviving and consuming, and therefore useful in more or less all areas. ‘Their use works on a two-sided basis: they are faster, better, more efficient and cheaper than people, but tactical, organizational and structural changes are necessary for their complete placement in the system’ (Notes, 2018). All robotization issues have not been resolved yet. One of them is how to control a robot –how to control a weapon that strives for a greater autonomy, how can we rely on the robot to be reliable in separating enemy units from soldiers.

‘The most recognizable unmanned aircraft are definitely drones, which are some kind of flying robots, similar to insects and capable of many things. In addition to transmitting cargo, observing, recovering, perceiving, shooting with various weapons, receiving commands at long distances and automatically avoiding obstacles they are also able to respond to hand gestures and follow their owner’ (The Economist, 2017), and to automatically switch to standby operation or transport position. Due to their versatility and relatively low prices, they are highly sought-after on the market and represent a cheap toy, a business opportunity and an expensive and dangerous weapon. Bunker, in a study entitled ‘Weapons Systems Life Cycles Analysis and New Strategic Realities’, claims that ‘armed robotic systems in the form of teleoperated, semi-autonomous and even autonomous drones and droids are not yet equipped with AI but are still operated by soldiers who use standard connections and control devices for management, while the more sophisticated are using wireless and satellite systems. In the near future, they will be equipped with AI and are likely to be able to respond independently and achieve some forms of self-awareness' (Bunker, 2017).

As in all areas, humans have always tried rationalising in the field of warfare. Therefore they always looked for a way and for means of defeating the opponent by using only the necessary forces and resources and resulting in the least number of victims. Today the first robots have entered the battlefields and many are eagerly waiting for it. It is true that robots reduce the need for people to carry out the tasks and that consequently brings fewer victims and in principle, there should be less collateral damage. On the other hand, this contests the traditional notion of being a soldier - the warrior and the mentality of the war. The management of the battle with remote machines and without the physical danger changes the mindset of the warfare. The forces of a technically inferior enemy and attacks on civilians give rise to abuse such as attacks from self-interest, etc. On the other hand, there is always the risk when such a weapon is separating a friend from the opponent, what if he breaks down or is injured and turns on us? How will we handle it and under what laws? It is true that machines must serve us, but we must control them, manage them, and take responsibility for their actions- the machine cannot protect our interests in the war. The machine can only be a tool and must remain a tool.

Nanotechnology

'The field of nanotechnology is defined as 'imaging, measuring, modelling and manipulating with substances in dimensions between about 1 and 100 nanometers', where unusual physical, chemical and biological properties can occur due to such low values also outside the Newtonian Physics Act' (EchevarriaII, 2009).This opened the way for new solutions to mechanical and biological problems that lead to completely new military capabilities. Due to the improved detection and decontamination capabilities, nanotechnology is located in many applications related to the defence against weapons of mass destruction and due to the required low power, low mass and low prices in handheld radio devices. Nanofibers are tested to seek better protection against chemical, biological, radiological, nuclear and high-energy explosive weapons or use in military uniforms and equipment.

The concept of equipment of a modern soldier states that this should be an integrated technological system that will provide the military with chemical, biological and ballistic protection, communication and information support, power, physiological control and climate control. All this additional protection, safety, greater survival and efficiency should be provided by nanomaterials. On the other hand, the question arises as to what happens when these matrices destabilize during combat, how they affect the environment and the soldier who uses this equipment. Is it an advantage or a weakness? What do all these implants and supplements mean for a soldier's long-term health and stability and are there also any side effects?

Biotechnology

‘One of the areas with enormous potential is biotechnology, which includes biometrics and genetic engineering and represents an area that is likely to be the next proclaimed war zone’ (Notes, 2018). Genetics determines our strongest physical characteristics such as height, eye colour, body shape, muscle strength and practically all other features of our physical structure, while also affecting our mind, psychical traits and talents. It’s not hard to imagine that by encroaching on our genetic design we could almost create people by a recipe. ‘Genetic engineering seeks to translate biological systems into engineering systems, transforming the army through biotechnology’ (Echevarria II, 2009). Soldiers Systems increase, ‘individual human abilities using artificial means such as robotic exoskeletons, smart textile, drugs, and seamless man-machine interface. Uses include capacity to endure extreme environments, better health monitoring and care provision, decision making at individual level’ (NATO STO, 2017).

Biotechnology is characterized by the use of organisms, tissues, cells, or molecular components of living beings to function and to act in such a way that they interact in the action of cells or their molecular components. This, in practice, means that biotechnology can increase the physical ability of a soldier to fight for longer under extreme conditions. Fewer soldiers are needed for the same task. The question is, however, how all these changes and 'defects' in the organism reflect human beings in the long run. It is true that biotechnology corrects the defects in organisms and corrects their genetic records. What does it mean for an organism when biotechnology 'breaks down'? What happens to a soldier when the fight is over, is it possible to return to a former state without any consequences? We will probably not get a real and honest answer to this question. It is always necessary to weigh what improvements bring, both positive and negative.

Cyberspace

‘In 2011, the US Defence Department declared cyberspace a new field of warfare; since then DARPA has begun a research project known “Project X” with the goal of creating new technologies that will enable the government to better understand and map the cyber territory’ (Wikipedia, 2014). Cyber-attacks cause greater damage to state authorities, business entities and critical infrastructure day by day, and are becoming frequently, better organized, difficult to manage and costlier. According to the NATO; ‘they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organized criminals, terrorist and/or extremist groups can each be the source of such attacks’ (NATO, 2010). Recognition of the cyberspace as a field of operation should include the current problem of different views and find a common position and agreement on a cyber-domain that would explain possible cyber operations. NATO is in Summit in Warsaw on July 2016; ’recognised cyberspace as a “domain of operations”, that cyber defence is part of NATO’s core task of collective defence, and that NATO is ready for the Allies to invoke collective defence in response to a significant cyber attack, equivalent of an armed attack through cyberspace’ (NATO CCDCOE, 2016).

This action additionally confirms the fact that cyberspace represents an environment in which there is a great possibility of implementing network operations and therefore it is urgent to be edited. Today's tendency is that more or less all systems are integrated into a single, common network, providing significantly faster, better quality and better data exchange, while simultaneously opening a new and vulnerable space for various cyber-attacks. These attacks are constantly increasing, both in terms of numbers and in terms of the depth and depth of their impacts, which poses a threat to the functioning of public and government information systems and the protection of data, as well as the functioning of banks and all other institutions that use the network, and therefore jeopardize their functioning, credibility and trust. This is why the question arises as to how to protect this proctor from cyber-attacks and whether this represents a new, completely digitized form of wars?

Implication on the armed forces

According to Margaret Kosal;

> The widespread enthusiasm for emerging technologies is reflected not only in official rhetoric but is also codified in respective national technology strategies and the global upswing of dedicated funding. Military-related programs in potential peer competitors in Asia (China), in states posing regional security challenges in the Middle East (Iran), in the former Soviet Union (Russia), and in rapidly developing areas (including South Asia, Southeast Asia, and Brazil) offer comparisons for advanced, allied states (U.S., Western Europe, Japan, ROK) in order to understand the national meanings, organization, and strategic implications surrounding the development and fielding of emerging technology (2016).

It should be emphasized that the integration of new technologies into armament platforms is a complex and multi-layered process. ‘There is no time for error on the battlefield. War is a matter of heart and will first, weaponry and technology second’ (Sullivan, 1993). The Centre for Strategic and International Studies (CSIS) wrote that we are entering an era in which:

> Computers are becoming faster and more ubiquitous, medical breakthroughs are prolonging and enriching lives and machines are becoming smaller by the day today. At the same time, as new technologies become embedded in our lives, we are forced to address issues of ethics, privacy, discrimination, and even basic human interaction. Technology will increasingly test the ability of individuals, cultures and governments to adapt to new opportunities and dangers (2018).

Success or failure of future conflicts will largely depend on how quickly and effectively different available technologies can be used on the current battlefield. All technologies will not have the same effect on the military field, and some will have a significant impact and will condition the future functioning of military systems, military planning and decision-making in the future. By changing the way forces are organized according to the available technologies, ‘we may be able to change the speed and extent of combat in the battlefield,’ (Orio, 2018). But science and development go ahead in all areas. Some large and rich countries have financial resources and invest in development, while others are looking for alternative solutions and responses to newly developed weapons through the action-reaction system.

The mission of deciding belongs to a human, not a machine

The future generations of military robots will operate more autonomously than comparable devices today, but will they be able to make decisions about life or death?

The technology means a lot, but not everything. In Rand, the relationship between technology and human beings has been written as;

> Technology cannot substitute for sociocultural, political, and historical knowledge. This knowledge is critical for understanding a conflict, formulating a strategy, and assessing its implementation. There has been a deficit of this knowledge, partly due to a continuing overreliance on technology and a belief that wars can be fought and won by reliance on technology alone. Without sociocultural, political, and historical knowledge, necessarily developed over time, the required adaptations in a strategy cannot be recognized and made (2014).

When we analyse the history of wars and battles we quickly find out that everything did not proceed in accordance with the 'rules', such as for example that in order to succeed it is necessary to ensure a ratio of forces of at least 3:1, that technological superiority also automatically means victory. For example, in the Second World War, the Nazi German Army was much better equipped than other armies and also used the tactics of 'blitzkrieg' tactfully. They developed modern tanks, planes, missiles, an atomic bomb, but despite all this technical advantage, they were not victorious. Similarly, in the Vietnam War where the US had the great technological power, it did not bring them victory. In Afghanistan, the highly modernized coalition troops are equipped with drones, reconnaissance robots and engineering and on the other side are the poor armed Taliban and their mine-explosive obstacles on the roads, which caused a lot of victims and material damage. All these examples show that despite military superiority, on the one hand, a person who is threatened, in distress and under pressure is always able to find an answer and an asset. A human is a being who thinks and acts and does not act after some recorded logs as a robot, but he feels, thinks and reacts outside these frames. This brings him progress and development in the field of tactics and the use of units, funds and counter-agents. And here a human is irreplaceable and it is the humans’ responsibility to prosecute the target.

We will use the robot as the soldier who will always appear first before the dangerous and invisible enemy. Antulio J. Echevarria II wonders:

> What laws and ethical codes will be needed to govern the use of such weapons? What signal or “message” do we send to those on the other side or to the international community when we send machines-rather than our own blood-to protect our interests in wartime (2009)?

However, human will be irreplaceable in the most difficult and most complex environments such as cities and the jungle. If robots' sensors and AI work flawlessly they should recognize and act automatically in front of an opponent or an intruder. What if they will not, what if their sensors receive distorted information and turn on us? The new technology does not only bring advantages it also brings its' weaknesses that military institutions have to face. This is also confirmed by Van Creveld when he says:

> The greatest victories that have been won in war do not depend upon a simple superiority of technology, but rather on a meshing of one side's advantages with the other's weakness so as to produce the greatest possible gap between the two (1991).

That is why we must understand technological changes and develop doctrinal rules that will solve the future questions of war. Technology should not become a guide, but it must remain useful as a service to use when it is needed and for the purpose, it is intended for. We must not become its' slaves, but we must learn how to manage it so it serves us. Lewis likewise considered: James Andrew Lewis also considers in a like manner. According to Lewis:

> Computers were invented to augment human performance. They are powerful tools, but even as processing speeds increase and algorithms grow more sophisticated, these machines still cannot "think." Eventually this will change. A group of leading scientists and public figures signed an open letter warning of the dangers of this moment. One famous scientist warned that "The development of full artificial intelligence could spell the end of the human race" (2018).

Soldiers are fighting wars in the name of politics, everything else are just tools and weapons that they use to eliminate the potential enemy and achieve the desired victory. With all these innovations, the attitude towards warfare is likely to change. After all, the question arises of what will be the role of men in the decision-making system, if everything depends on the computer and what will this supercomputer decide to be superfluous?

Conclusion

Increasing the power of some countries and the availability of new technologies further increases the complexity of the environment. War and clashes of the past have shown that technology has changed the mode of warfare. Strategies and tactics are changing due to new technologies. These technologies will have an impact on future kinetic and non-kinetic operations. For this reason, today's' military planners and developers must think systematically about the possible future development of technology. This process should not be limited to technology but must include possible future weapons systems and military equipment, hybrid threats and social changes that can occur with technological development.

Equipment, weapons systems, tactical and strategic ideas, doctrines and the structures of the armed forces are being changed. The way of complementing the armed forces, the educational structure, age structure, social and sexual structure is changing. On the one hand, the structure of the armed forces reflect the attitude of the society towards them and on the other hand, the needs of the armed forces. Scientific and technological progress has a significant impact on the armed forces. It offers them a more efficient mode of operation, better protection against the enemy, simplifying the process of weapons production, allowing greater control of the battlefield and providing improvements that create the difference between defeat and victory. However, this requires well-trained individuals who are able to manage increasingly sophisticated systems. Being trained means not only in physical fitness but also in some mental abilities and a wealth of knowledge. As scientific and technological advances allow and at the same time require the involvement of highly educated personnel. Scientific and technological progress brings many direct innovations, such as armaments and support systems, into the armed forces, but it also brings indirect changes that arise mainly from the characteristics of the operation of these systems. Modern armament systems require knowledge of the systems and the importance of physical power decreases. Indirectly, scientific and technological progress has led the whole world to become a potential battlefield, which means that there is no clear separation between the front and the hinterland. At the same time, there is very little or no direct physical contact, even less visual contact, the personal image of the enemy is lost. Scientific and technological progress alters the operational, tactical and strategic ideas of the armed forces of the modern industrial states. In order to succeed, we must know very well the abilities and capabilities of technology, their tactical and technical abilities and use it accordingly. This can bring us an advantage and success. The massive and all-around non-intrusive use of technology does not ensure success. As Albert Einstein once said about the explosion of an atomic bomb; ‘I **know not** with what **weapons World War** III **will** be fought, but **World War** IV **will** be fought with sticks and stones' (Brainyquote, 2001). This suggests that our technology must remain the same, primitive.

Bibliography

Brainyquote. 2001. Albert Einstein Quotes [Online] 2001. [Cited: 20 March 2018.] https://www.brainyquote.com/quotes/albert_einstein_122873?src=.

Bratanič, Jan. 2018. Technology strengthens the best and the worst in humans. *Svetkapitala*. [Online] January 2018. [Cited 20 March 2018.] https://svetkapitala. delo.si/inovacije/tehnologija-krepi-najboljse-in-najslabse-v-ljudeh-4616.

Brimley, Shawn, Hendrix, Jerry, Fish, Lauren, Routh, Adam and Velez-Green, Alexander. 2018. Building the Future Forces. *CNAS.* [Online] 29 March 2018. [Cited 12 April 2018.] https://www.cnas.org/publications/reports/building-the-future-force.

Bunker, Robert J. 2017. Armed Robotic Systems Emergence: Weapons Systems Life Cycles Analysis and New Strategic Realities. *Strategic Studies Institute and U.S. Army War College Press*. [Online] 14 November 2017. [Cited 12 March 2018.] https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1368.

CSIS. 2018. Revolution 3: Technology. *Centerfor Strategic and International Studies*. [Online] 28 August 2015 [Cited: 12 April 2018.] https://www.csis.org/programs/international-security-program/strategic-futures/revolution-3-technology.

Çalişkan, Murat and Liégeois, Michel. 2017. Technology and War Strategy. *Beyond The Horizon*. [Online] 13 June 2017. [Cited: 17 March 2018.] https://www.behorizon.org/technology-and-war-strategy/.

Echevarria II, Antulio J. 2009.Strategic Implications of Emerging Technologies. *U.S. Army War College, Strategic Studies Institute*. [Online] [Cited: 14 March 2018.] https://ssi.armywarcollege.edu/pdffiles/PUB927.pdf.

Evans, Dave. 2010. Top 25 Technology Predictions from Futurist Dadve Evans. *Techvibes*. [Online] 4 March 2010. [Cited: 8 March 2018.] https://techvibes.com/2010/03/03/top-25-technology-predictions-from-futurist-dave-evans.

Kosal, Margaret. 2016. Science, technology, and the future of warfare. *Modern War Institut*e. [Online] October 2016. [Cited: 30 January 2018.] https://mwi.usma.edu/science-technology-future-warfare/.

Lewis, James Andrew. 2018. Waiting for Skynet. *Center for Strategic and International Studies.* [Online] 18 January 2018. [Cited 12 April 2018.] https://www.csis.org/analysis/waiting-skynet.

Meyer, David. **2017.** Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World. *Fortune.* [Online] 4 September 2017. [Cited: 20 March 2018.] http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/.

NATO. 2010. Strategic Concept. *NATO Public Diplomacy Division*. [Online] February 2012. [Cited: 20 March 2018.] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

NATO CCDCOE, 2016. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. *NATO CCDCOE*. [Online] 21 July 2016 [Cited: 17 March 2018.] https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

NATO RTO, 2011. Joint Operations 2030 – Final Report. *NATO RTO*. [Online] 1 June 2014 [Cited: 18 March 2018.] https://www.researchgate.net/publication/229428350_Joint_Operations_2030_-_Final_Report.

NATO STO. 2017. STO Tech Trends Report 2017. Public Release Version of AC/323-D(2017)0006 (INV). *NATO Science & Technology Organization.* [Online] 15 September 2017. [Cited: 8 March 2018.] https://www.sto.nato.int/SitePages/newsitem.aspx?ID=3534.

Orio, Brendan. 2018. Order from Chaos: Six technologies that the U.S. military is betting on. *Brookings*. [Online] 28 January 2018. [Cited: 25 February 2018.] https://www.brookings.edu/blog/order-from-chaos/2016/01/28/six-technologies-that-the-u-s-military-is-betting-on/.

Rand. 2014. Lessons from 13 Years of War Point to a Better U.S. Strategy. *Rand*. [Online] 2014. [Cited: 12 March 2018.] https://www.rand.org/pubs/research_briefs/RB9814.html.

Roland, Alex. 2009. War and Technology. *Foreign Policy Research Institute.* [Online] 27 February 2009. [Cited] 10 March 2018. https://www.fpri.org/article/ 2009/02/war-and-technology/.

Schwab, Klaus. 2016. The Fourth Industrial Revolution. World Economic *Forum.* [Online]. [Cited: 25 February 2018.] https://www.weforum. org/pages/the-fourth-industrial-revolution-by-klaus-schwab.

Straub, Jeremy.2018. Artificial intelligence is the weapon of the next Cold War. *The Conversation*. [Online] 29 January 2018. [Cited: 20 March 2018.] https://theconversation.com/artificial-intelligence-is-the-weapon-of-the-next-cold-war-86086.

Sullivan, Gordon R. and Dubik, James M. 1993. Land Warfare in the 21st Century. *U.S. Army War College Strategic Studies Institute*. February 1993. [Online] [Cited: 17 March 2018.] http://ssi.armywarcollege.edu/pubs/1993/landwar/ landwar.pdf.

The Economist. 2017. Commercial drones are the fastest-growing part of the market. [Online] 10 Jun 2017. [Cited: 22 March 2018.] https://www.economist.com/news/technology-quarterly/21723003-most-drones-today-are-either-cheap-toys-or-expensive-weapons-interesting.

Van Creveld, Martin. 1991. Technology and War: From 2000 B.C. to the Present. *Simon and Schuster*. [Online] May 2010. [Cited 20 March 2018.] https://books.google.ee/books?hl=sl&lr=&id=A7FZ98dFQbkC&oi=fnd&pg=PR9&dq=technology+and+war&ots=1j_SsQK8ZX&sig=IPY94hgu9bIgniLQEYKbNQZE79Q&redir_esc=y#v=onepage&q=technology%20and%20war&f=false.

Wikipedia. Cyberspace. *Military Technology*. [Online] 2014 [Cited: Cited: 12 March 2018.] https://en.wikipedia.org/wiki/Military_technology.

Žabkar, Anton. 1994. Research and development policies and the costs of NATO - after the Cold War. Theory and Practis. *FDV*. [Online] 2000 [Cited: 7 February

2018.] https://www.dlib.si/stream/URN:NBN:SI:doc-1P5ISSOH/5aea4216-ca25-4f39-a327-53e2866c4f68/PDF.

Notes:

Notes, 2018. Personal notes from lectures HSCS 2018, January - June 2018 in the Baltic Defence College.