Resilience: Silver Bullet in Challenging Hybrid Warfare?

Christoph Bilban, BA

This paper examines the concepts of resilience and hybrid warfare, which both recently became popular in security policy as a result of the crisis in Ukraine. Resilience is proposed as a counter-strategy against hybrid threats. Reviewing recent literature and policy papers, the author argues that resilience can be a counter-measure to certain subsection of hybrid warfare, shown by the example of information warfare. This paper points out however that strategies nowadays labelled as *resilience* have been in existence in one form or another since the Cold War era.

Keywords: resilience, hybrid warfare, deterrence, information warfare, Russia

Ever since the Ukraine crisis struck Europe, many scholars have been calling for more resilient security policies, both on the European and national levels. They argue that resilience is the "magic bullet" to counter hybrid warfare and the threat posed by Russia. In most of these papers, resilience seems to be little more than a buzzword, though: Scholars from different fields of study are still trying to come up with a common understanding of what resilience is or should be. The recent debate on resilience is centring on two notions: bounce back and restore, or adapt and thrive. As the concept allows for a wide range of interpretations, it became a buzzword in many national security strategies, especially in terms of critical infrastructure protection (CIP). That is not surprising, as CIP mostly deals with technical details on how to prevent critical infrastructures such as power gridsor communication networks from failing under external duress. Many policy papers however emphasise making the population more resilient towards disasters, emancipating communities to take responsibility for their well-being in times of crisis. Brassett, Croft and Vaughan-Williams (2013) in their introduction to a special issue of *Politics* focused on *resilience* state that "resilience seems to carry a productive ambiguity that both resists exact definition and allows for a spectrum of interactions and engagements between policy and the everyday which are as (seemingly) effective as they are (apparently) apolitical" (p. 221). Some scholars even argue that resilience per se is a neoliberal concept (for example Joseph, 2013), meant to enable the retreat of the state from its very purpose – providing security. On the other hand, the Ukraine crisis seems to have resurrected not only NATO but also the nation state as a security provider. As the term *hybrid warfare* is making the rounds in the security policy discourse, it was to be just a matter of time until someone argued in favour of resilience as a defensive concept in a *hybrid* threat environment. This paper will outline the circumstances under which resilience could become a defensive strategy to such threats. I will argue that both resilience and hybrid warfare have a common ground in their underlying logic

of function. In the following section, I examine the development of the term resilience. Then, it will be necessary to define hybrid warfare, its nature and overall relevance as an analytical term.

Resilience and security

As early as 2013, Pospisil argued that resilience would eventually become an enticing concept for security policy (p. 29). Linking resilience with risk, he deemed possible a fundamental reconfiguration of security policy through the resilience paradigm (p. 26). However, the origins of the term *resilience* are still unclear. Until today many scholars (for example Brassett, Croft & Vaughan-Williams, 2013; Pospisil, 2013; Bourbeau, 2013; McAslan, 2010) refer to the Latin root of *resilentia*, which describes "[t]he action or an act of rebounding or springing back" (Oxford dictionary as cited in Pospisil, 2013, p. 28). McAslan (2010) has tracked the first use of resilience in scholarly work to the early 19th century, when the concept of resilience was used "as a means of measuring and comparing the strength of materials used in the construction of Royal Navy's fighting ships" (p. 2). Both Pospisil (2013) and McAslan (2010) also refer to the work of Holling from 1973, who introduced the concept of resilience in ecology and environmental science. Holling was the first to integrate resilience with systems theory. In his view resilience is defined "as the measure of its ability to absorb changes and still exist" as McAslan (2010, p. 3) puts it. Holling opposed the concept of resilience to stability of ecological systems. While stability implied the existence of an equilibrium and its sustainment in times of crisis, resilience had a dynamic approach focusing on constant adaptability and persistence of the system.

Pospisil (2013) argues that this dynamic notion of resilience is closely linked to idea of a *risk society*, which Beck described. Risk has, according to Pospisil (2013), three functions in the changing character of security policy: extending the notion of *security*, introducing uncertainty and unknowingness, and a shift in responsibility and agency, as the state no longer remains the sole provider of security (p. 30). According to Brassett, Croft and Vaughan-Williams (2013) the rise of resilience in international relations "has gone hand in glove with the rise of the risk-related research and analyses of contemporary attempts to *live with* rather than *overcome* global uncertainties" (p. 223).

First concepts of *comprehensive security* emerged in the 1990s and after the pivotal events of 9/11, the discourse about security eventually incorporated demography, financial architecture, technology or even "ways of life", all fields that had seemed somewhat remote in prior decades (Brassett, Croft & Vaughan-Williams, 2013, p. 223). A state of uncertainty challenged the

classical notion of security, one where states encountered risks by clearly defining and combatting them. Today, security policies are more concerned with the inherent vulnerabilities of a state. Pospisil (2013) mentions that this altered understanding led to a shift in responsibilities (p. 30). Whole-of-nation approaches subsequently occurred and the role of governmental agencies in security provision diminished, at least in theory. However, in his article Pospisil (2013, p. 33) accentuates the fact that by 2013, resilience, in terms of "hard" security, was present only in domestic security. The military section of international security debates was not yet significantly influenced by the concept of resilience, except for various NATO documents on critical infrastructure protection and cybersecurity. A reason for this asymmetry was the absence of a clear threat or enemy to address for military to create realistic threat scenarios, argues Pospisil (2013, p. 34). He may have been right, as resilience experiences a steep career since the comeback of a perception of a looming threat emanating from Russia starting in 2014.

McAslan (2010), too, contemplates the relationship of resilience and security. He mentions that resilience and national security have common roots and requirements, despite significant differences in other areas (p. 8). Threat and vulnerability assessment is perceived as the intersection of resilience and national security; the major difference is their approach to deal with respective threats. Security on the one hand figuratively moves into a defensive posture, trying to block and defeat threats. Resilience meanwhile yields to the omnipresence of threats and is aware that some may become disruptive events. Hence, resilience aims at reducing the impact of events and recover afterwards, but not necessarily to prevent them. (McAslan, 2010, p. 8)

Pospisil (2013) follows up this idea, concluding that resilience aims at creating a state of freedom under the premises of constant risk (p. 38). Security is no longer the sole preserve of the state. According to the political scientist Herfried Münkler (as cited in Pospisil, 2013, p. 38) modern societies risk self-destruction if they tend to maximize security beyond a certain level. McAslan exemplifies how disproportionate safeguarding efforts by the state threaten resilience of a society, quoting Templeman's and Bergin's seminal paper on the resilience of Australia. "We've come to believe that our workforce of emergency volunteers will always be there to manage all hazards … it's very difficult for individuals and some business organisations to comprehend that they might be affected" (Templeman & Bergin as cited in McAslan, 2010, p.9).

Hence, the rise of resilience was accompanied by a radical shift of security logics. Brassett, Croft and Vaughan-Williams (2013) in their article refer to Mark Duffield who argued that the emergency planning of the late twentieth century was based on the prediction of events, isolation and relocation of threats and the protection of the society, using military and quasi-military means. In stark contrast, nowadays resilience requires society to learn new skills and be prepared as to be able to "exploit the emergent opportunities that disorder inevitably creates" (Duffield as cited in Brassett, Croft & Vaughan-Williams, 2013, p. 223).

McAslan (2010) continues to work out seven previously discussed characteristics of resilience. First of all, resilience always refers to some threats or dramatic events, which have a potentially overthrowing impact to a system. Secondly, resilient systems strive for a positive outcome, be it either the restoration of the status quo or change and improvement. These two outcomes are commonly known as *bounce back* or *adaptation*. Thirdly, resilient systems need to be prepared either by standards, operational procedures, human or social capital, et cetera. Meanwhile, preparedness is but one important aspect of resilient systems, as they need to be willing and able to adapt to a constantly changing environment. Adaptability hence is the fourth characteristic of resilience. Fifth comes the willingness to learn and gain experience. Coordination and interdependency is sixth, meaning resilient systems and nations "tend to be those which are well coordinated and share common values and beliefs" (p. 10). The core belief, and seventh characteristic of resilience, is the desire to survive. These characteristics make the concept of resilience "a powerful and useful concept", McAslan concludes (2010, pp. 10-11).

Besides being a powerful concept, critics argue that resilience is inherently neoliberal as society is in a constant state of emergency and threats are ubiquitous. Brassett, Croft and Vaughan-Williams (2013, p. 224) argue that uncertainty becomes the starting point for neoliberal governance. The incapacity of the nation state to provide security to every individual, community or business necessitates that these subjects manage their own risks. Jospeh (2013) goes as far as to argues that the subjects are indeed encouraged to "take responsibility for their own social and economic well-being" rather than relying on the state. He goes on to focus on the risk and security aspects of a neoliberal way of governance encouraging "preparedness and awareness" (p. 42). While resilience promotes a concept of active citizenship, it doesn't ultimately issue any guarantees. Dunn and Prior (2013) argue, that resilience "currently enjoys an international status as a panacea for modern security challenges, as it leaves room for a new kind of subjective perception of security, despite the unpredictable nature of contemporary hazards" (p. 3).

Up to this point, I discussed the notion of resilience from a general perspective, trying to understand what the concept of resilience encompasses. I conclude that resilience basically divides into either *bounce back* or *adapt*. Furthermore, it seems that resilience is binary in nature, either in existence or not. This notion, however, is challenged by Bourbeau (2013) as resilience from his point of view "is always a matter of degree" (p. 11). Resilience is described more like a process, one that never will quite complete Another dichotomy and inherent contradiction within resilience is addressed by O'Melly (2010). He states that many definitions either imply a reactive or proactive account of resilience. Approaching the concept of resilience from a psychological perspective, he analyses how military psychiatry treats and tries to prevent cases of PTSD with military personnel, then further addresses the conjunction of resilience and warfare in liberal societies. He refers to the work of Dillon and Reid[1], who assume that "the necessity of recognizing that life is in its nature uncertain – has had a profound impact both on liberal rule and liberal warfare" (O'Melly, 2010, p. 501). This uncertainty shaped the new military need for a governance of "these labile and evolving potentialities […] [by, CB] a flexible and adaptive military government" (p. 502). In modern warfare, the symmetrical, regulated battlespace dissolves as "each side plays according to its own rules and seeks weakness wherever it can be made to appear" (p. 502). For Dillon and Reid, *network-centric warfare* (NCW) represents the changes in the military arena as "information and communication are pivotal organizing principles and prime movers, in which weapons […] transformed from entities with stand-alone capabilities into relational elements whose potential lies in their place in a complex, adaptive and emergent open system" (Dillon & Reid as cited in O'Melly, 2010, p. 502).NCW however evolved from a bigger societal shift provoked by "the dynamics of growth and competition that have emerged in the modern economy" (Alberts as cited in O'Melly, 2010, p. 504). Dillon and Reid go even further as they argue that "the laws which were to govern the development of this liberal way of war were in essence indistinguishable … from the laws which governed the development of the liberal way of living as such" (Dillon & Reid as cited in O'Melly, 2010, p. 504). O'Melly (2010) addresses the afore mentioned neoliberal character of resilience, one that shifts responsibilities to the lowest level possible. Resilience thus has become a technique to enable "the subject to deal with uncertainty *in general* [and not specific threats, CB]" (p. 505).

[1] The cited opus is Dillon, M. & Reid, J. (2009). *The liberal way of war: Killing to make life live*. London: Routledge

Hybrid warfare – Neither new, neither Russian

This high level of uncertainty undoubtedly contributes to the term *hybrid warfare* becoming wildly popular among scholars, practitioners and pundits ever since the Russian annexation of the Crimean Peninsula in 2014. Yet the very concept of hybrid warfare is hardly novel. The American scholar Hoffmann described it in 2007 using the example of Hezbollah during the Israeli-Lebanese war in 2006. Murray and Mansoor (2012) follow the traces hybrid warfare left over the course of more than 2.000 years of warfare. They define hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents, and terrorists), which could include both state and nonstate actors, aimed at achieving a common political purpose" (p. 2). In fact, it was Clausewitz who stated that every war serves a political purpose (1995 [1832]). According to him, war is always an instrument of politics, and therefore war is constantly changing faces from conflict to conflict. Clausewitz already hinted about technology's impact on war, but concluded that his very nature remains the same. Following this assumption, one could now conclude that the rise of information technology is a *revolution in military affairs* (RMA), but did not significantly alter the nature of war itself. The same must be true for *hybrid warfare*, as *hybrid* merely refers to the means and actions taken.

It is obvious now that Russia is not the inventor of hybrid warfare. At theWales Summit NATO "put the issue of hybrid war in the specific context of the Russia/Ukraine crisis" (Giegerich, 2016, p. 66). Even though scholars tried to implement labels like "full-spectrum conflict" (Jonsson & Seely 2015), the term *hybrid war(fare)* is used as a synonym for Russia's military and non-military involvement in Eastern Ukraine, yet its coverage often remains vague and indistinct. Russian scholars now also use the term *gibridnaya voyna*, despite having used terms like "new generation warfare", "sixth generation warfare" or "non-linear war" before.

Diego Ruiz Palmer (2015) of NATO Defence College explicates that the *scale* "sets Russia's hybrid warfare apart" (p. 1) from other forms of asymmetric war. Additionally, Russian hybrid warfare "bridges the divide between hard and soft power applications that result from the technological and information revolutions […] in ways that maximize asymmetric advantages to Russia" (p. 2). For Ruiz Palmer (2015) Russian hybrid warfare is the result of a transformational process that was started already in the Soviet armed forces, which even then conceptualised *"*21st century, distant, 'no-contact warfare'*[NCW]*" (p. 6). This transformation has its roots in the concept of *deep operations*, aiming to hit the enemy on their territory and keep them away from the then-Soviet Union, or employ IRBMs. The pivot towards NCW in

the United States made Russia realise that the information space would have to be integrated into the concept of deep operations (p. 7). Ruiz Palmer (2015) concludes that the Russian revolution in military affairs is the

> *"conceptualization of the dynamic interaction between hard and soft power as a new form of war that extends the military contest to society as a whole. This makes hybrid warfare in the early 21st century an accomplished form of 'control war' over the ends, ways and means of nations, communities and societies" (pp. 7-8).*

This understanding of hybrid warfare as a "control war" is also present in the Baltic states. As early as in April 2014. Janis Berzins of the Latvian Defence Academy drew conclusions for Latvia's national security in the light of Russia's "New Generation Warfare". His arguments originate from an essay[2] by General Valery Gerasimov (2013), which is considered to be theoretical cornerstone of Russia's hybrid warfare, as well as from a lesser-known article of Chekinov and Bogdanov (2013). Valery Gerasimov in his essay initially argued on the relevance of a highly educated and well-staffed General Staff, stating"[a]ny academic pronouncements in military science are worthless if military theory is not backed by the function of prediction" (Gerasimov as cited in Galeotti, 2014). Gerasimov ultimately agrees with Clausewitz on the fact that each war has its own face and needs its own strategies. The remarkable proposition of the so-called *Gerasimov doctrine* however is that "[t]he role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness" (Gerasimov as cited in Galeotti, 2014). Gerasimov directly refers to the Arab Spring as the model of 21st century warfare, where focus has shifted from traditional military to new methods (see Figure 1). He concludes that "contactless actions against the enemy are becoming the main means of achieving combat and operational goals" (Gerasimov as cited in Galeotti, 2014). The quiver of possible actions is well-stocked with "special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions" (Gerasimov as cited in Galeotti, 2014).

[2] The essay has been translated by Mark Galeotti (2014), who attached some commentaries. I will use his translation in this paper.

Figure 1 - Traditional vs. New Military Methods (Gerasimov as cited in Berzins, 2014, p. 4)

Traditional Military Methods	New Military Methods
▪ Military action starts after strategic deployment (Declaration of War). ▪ Frontal clashes between large units consisting mostly of ground units. ▪ Defeat of manpower, firepower, taking control of regions and borders to gain territorial control. ▪ Destruction of economic power and territorial annexation. ▪ Combat operations on land, air and sea. ▪ Management of troops by rigid hierarchy and governance.	▪ Military action starts by groups of troops during peacetime (war is not declared at all). ▪ Non-contact clashes between highly maneuverable interspecific fighting groups. ▪ Annihilation of the enemy's military and economic power by short-time precise strikes in strategic military and civilian infrastructure. ▪ Massive use of high-precision weapons and special operations, robotics, and weapons that use new physical principles (direct-energy weapons – lasers, shortwave radiation, etc). ▪ Use of armed civilians (4:1 civilians to military personnel). ▪ Simultaneous strike on the enemy's units and facilities in all of the territory. ▪ Simultaneous battle on land, air, sea, and in the informational space. ▪ Use of asymmetric and indirect methods. ▪ Management of troops in a unified informational sphere.

Berzins (2014) suggests that Latvia is already in Russia's crosshairs, and first "combat action" e in the information space has already commenced. He states that "the Russian view of modern warfare is based on the idea that the main battlespace is the mind" (p. 5). In their article, Chekinov and Bogdanov (2013) support Berzins' argument, claiming that information superiority will be crucial to reach one's objectives in a new generation of warfare. They refer to the US Army concept of network-centric warfare as the fundamental basis of any new generation warfare. Chekinov and Bogdanov understand NCW merely as a "concept to manage combat operations of different armed groups" (p. 18). Nevertheless, they argue that based on NCW, US-troops in the event of a new generation war will aim at quickly decapitating an enemy by eliminating his command, control and information (C2I) infrastructure. Their "innovation" is that the decapitation should not be limited to an enemy's C2I infrastructure, but aim at the nation as a whole. "Massed propaganda is used to provoke unrest within the population and soldiers […] in order to make people give up their resistance and achieve the disorganization of the political and military command" (Chekinov & Bogdanov, 2013, p. 20). According to Berzins (2014), the article of Chekinov and Bogdanov schematizes eight phases of new

generation warfare, developing from a non-military asymmetric warfare in the first phase to the "roll over [of] the remaining points of resistance […] and territory mopping-up operations by ground troops" in the eighth (p. 6).

Russian hybrid (or new generation) warfare is in essence a war against governability, as Mark Galeotti outlined in an interview (Manea, 2015). Especially all actions below the threshold of conventional war are aimed at creating unrest, provoking riots and general disorganization, mostly by large scale disinformation campaigns. Galeotti states:

> *"It is not about convincing anyone else of a Russian point of view so much as to undermine people's belief in any point of view, to create an environment in which no one can be quite sure about anything. […] Ultimately, hybrid defense is about legitimate and effective governance. On so many levels this is precisely a war of governance"* (Galeotti as cited in Manea, 2015).

This war on governance is hardly new when compared to what George Kennan outlined in 1948 on what he called *political warfare*:

> *"In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. […] The range from such overt actions as political alliances, economic measures, and 'white' propaganda to such covert operations as support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states"* (Kennan as cited in Siegert, 2016, p. 23).

Kennan's definition bears striking similarities with what is discussed as hybrid warfare thus far. Subsequently, hybrid warfare, neither the plain concept, nor the Russian derivation, are of groundbreaking novelty. So where does the anxiety stem from? The events in Ukraine exposed a latent conflict between different systems of values and beliefs. For one, Russia's stability is inextricably linked to foreign policy, particularly to be the hegemon in the Near Abroad (the former USSR). Russian understanding of external threats, meanwhile, are based on "the perception that Western democracy as such is a threat to Russia" (Blank as cited in Jonsson & Seely, 2015, p. 9). Last but not least, Russia feared a possible loss of its naval base in Sevastopol due to the regime change in Kiev. While the operation in Crimea ran smoothly, the uprising in Eastern Ukraine turned out to be an enduring, violent disarray of vast regions. Nevertheless, the swift and artful annexation of Crimea did not fail to make a stark impression on Europe and NATO. The West realized that its societies, too, are vulnerable to destabilization by hostile agents and (dis)information campaigns, and furthermore that territorial integrity might no longer be assured by international agreements. Simply put, "hybrid warfare" developed from a concept of mainly academic value ato a significant and tangible risk to Western societies.

Resilience to counter hybrid warfare?

This perception of high risk posed by hybrid threats, underlined by impressions from the Ukraine crisis, led to calls for resilience as the centrepiece of national and European security strategies. Major and Mölling (2014) claimed that "EU and NATO must place systematic vulnerabilities at the center of a hybrid security policy, which should build upon a reorganized relationship of resilience, deterrence, and defense" (p. 1). Resilience in their essay follows the notion of *bouncing back*. European societies should be able to recover quickly from attacks to either their values or every day functioning (p. 3). Resilience further means *preparedness* through redundancies, alternative supply chains and diversification of energy supply sources (p. 4). Hamilton (2015) also demands new "approaches […] that blend traditional efforts at deterrence with modern approaches to resilience, thus building a society's capacity to anticipate, preempt and resolve disruptive challenges to its critical functions" (p. 45).

In 2015, the EU started to work on a new security strategy: Resilience plays an important role there as well, illustrated by the following key recommendation:

> *"**Prioritise threats based on impact assessment and resilience.** The ESS should prioritise the set of threats Europe faces in terms of the severity of the impacts and decide how to respond through the lens of societal resilience. Such an approach can be made to work for a wide range of threats and so can be highly cost-effective. Resilient societies that have built-in ways and means to absorb or spread shock will manage their responses far more effectively than ill-prepared, more fragile communities" (Anthony, Grand & Lewis, 2015, p. 81).*

Furthermore, the briefing paper focuses on the resilience of European cyber space:

> *"The technical capabilities not only extend to non-state armed groups but also to individuals; thus the control over cyber technologies will remain severely limited in free and democratic societies. […] Understanding the risks (the combination of probability and consequence) and creating an in-built resilience will not only serve to protect against cyber-attacks but will also decrease the desirability of key targets and therefore also serve to deter" (Anthony, Grand & Lewis, 2015, p. 25).*

In this briefing paper resilience yet remains confined to playing a role in countering ecological threats, man-made catastrophes and the contingencies in cyber security. The value of resilience in the context of hybrid warfare seems to not have been acknowledged to date.

When it comes to resilience as a conceptual innovation to counter hybrid threats, this means *"foremost […] reducing one's own vulnerabilities"* (Giegerich, 2016, p. 69). Giegerich (2016) goes as far as to argue that "[while] doing so makes it less likely that hybrid attackers manage to achieve their intended goals, resilience also contributes to deterrence […] by reducing the potential gains any attacker might hope to reap" (p. 69).

Disinformation and propaganda, both centrepieces of hybrid warfare, pose a significant challenge to societal overall stability and resilience, if the latter is understood as marginality as described by Bourbeau (2013, pp. 14-16). Resilience as marginality is "aiming at keeping the changes produced by a crisis or shock as marginal in order to safeguard against changes to existing structures or policies" (Fjäder, 2014, p. 121). This notion of resilience, contradicts the nature of information warfare, which aims at shattering existing beliefs and value systems. In an open society, resilience of mind-sets shouldn't aim at bouncing back, but at renewal and constant discourse. The concept of resilience thus means to strengthen social cohesion by constantly pointing out the advantages of Western values and liberalism, while applying self-criticism at the same time. External shocks, for instance propaganda campaigns (e.g. the case of the German girl Lisa in early 2016), then should become the initial point for societal debates on values in order to build confidence in the nation state and the European Union. Berzins (2014) stresses that the success of the first two phases of hybrid warfare "determines the implementation of the following phases" (p. 7). These phases encompass information, moral, psychological and ideological measures targeted at the society as a whole and selected political and military personnel as well. Mölling argues, that a hybrid security strategy could put the EU in the position of countering "adversaries in the non-military arena to prevent an escalation toward military force" (Mölling as cited in Giegerich, 2016, p. 70). As a consequence, the first line of defence must be the buildup of a resilient collective mindset, which is able to withstand disinformation without cutting off freedom of speech or using indoctrination.

To implement such psychological resilience, most European member states would do well to recall their practices and procedures of psychological defence from the Cold War era. Andersson (2015) states that "a society's ability to defend itself crucially depends on its population having a critical mind" (p. 4). Source criticism can and must be taught in schools, and in particular at colleges of journalism. While Andersson (2015) describes a quite developed systems of psychological defence in Sweden during the Cold War, Austria at that time professed to a concept of all-encompassing defence ("*Umfassende Landesverteidigung*") consisting of four distinct pillars: military, civil, economic and psychological. Therein however, the pillar of psychological defence never was quite as appreciated as the other three. Its legal basis was not founded until 1994, when the Ministry for Education issued a decree on political education. Political education however is not only of concern in schools, but also and in particular in the military, regardless of being a professional body or one comprised of (mainly) conscripts. Uwe Hartmann (2015) outlined the relevance of the German Armed Forces' concept of *Innere Führung*, which is hard to paraphrase, but could be best described as *citizen in uniform*. Political

education and responsibility for one's actions lie at its very core. Hartmann underlines the importance of political education and open debates for politicians, society and soldiers in a hybrid war environment (pp. 88-104). In this light, reinforcing the European peoples' mindset is an imperative that seems all but obvious.

Summary

In this paper, I tried to clarify the notion of two frequently used terms in current security discourse: *resilience* and *hybrid warfare*. Hybrid warfare fits well with the concept of a risk society, as it hints at constant insecurities. The term resilience is derived from the same conceptual background and its emergence should thus not surprise. In this paper, I argued that resilience can be a strategy to counter certain so-called hybrid threats, especially those appearing in the cyber and information domain. Deterrence is difficult to achieve in these spheres, and resilienceat least promises to lower the effects of hybrid attacks whileat the same time raising the cost for an attacker.I do however agree with Major and Mölling (2015) who proposed a trinity of resilience, deterrence and defence to meet hybrid adversaries: No resilience-themed strategy can be sustainable without elements of hard power, i.e. well-equipped and well-trained armed forces, be they under a host of national commands or united under a joint European authority.

References

Andersson, J. J. (2015). Hybrid operations: lessons from the past. *ESS Brief Issue*, (33).

Anthony, I., Grand, C., & Lewis, P. (2015). *Towards a new European security strategy? assessing the impact of changes in the global security environment.* Luxembourg: Publications Office. Retrieved from http://bookshop.europa.eu/uri?target=EUB:NOTICE:QA0115422:EN:HTML

Berzins, J. (2014). Russia's New Generation Warfare In Ukraine: Implications For Latvian Defense Policy. *Policy Paper No. 02*. Riga: National Defence Academy of Latvia Center for Security and Strategic Research.

Bourbeau, P. (2013). Resiliencism: premises and promises in securitisation research. *Resilience*, *1*(1), 3–17. doi:10.1080/21693293.2013.765738

Brassett, J., Croft, S., & Vaughan-Williams, N. (2013). Introduction: An Agenda for Resilience Research in Politics and International Relations: Agenda for Resilience, an Introduction. *Politics*, *33*(4), 221–228. doi:10.1111/1467-9256.12032

Chekinov, S. G., & Bogdanov, S. A. (2013). О характере и содержании войны нового поколения [About the chracter and meaning of new generation warfare]. *Voennaya Mysl'*, (10), 13–24.

Clausewitz, C. von (1995). *Vom Kriege: Auswahl* (Nachdr.). Stuttgart: Reclam.

Dunn Cavelty, M., & Prior, T. (2013). Resilience in Security Policy: Present and Future. *CSS Analysis in Security Policy*, (142).

Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience*, *2*(2), 114–129. doi:10.1080/21693293.2014.914771

Galeotti, M. (2014). The "Gerasimov Doctrine" and Russian Non-Linear War. *In Moscow's Shadows*. Retrieved from https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Gerasimov, V. (2013). Ценность науки в предвидении [The value of science in prediction]. *Voenno-Promishleny Kurer*, pp. 1–3. Moscow.

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections: The Quarterly Journal*, *15*(2), 65–72. doi:10.11610/Connections.15.2.05

Hamilton, D. S. (2015). Rude Awakening: Security Challenges in Northern Europe. In N. Hvidt & H. Mouritzen (Eds.), *Danish foreign policy yearbook 2015* (pp. 25–50). Copenhagen: DIIS.

Hartmann, U. (2015). *Hybrider Krieg als neue Bedrohung von Freiheit und Frieden: zur Relevanz der Inneren Führung in Politik, Gesellschaft und Streitkräften*. Berlin: Carola Hartmann Miles-Verlag.

Jonsson, O., & Seely, R. (2015). Russian Full-Spectrum Conflict: An Appraisal After Ukraine. *The Journal of Slavic Military Studies*, *28*(1), 1–22. doi:10.1080/13518046.2015.998118

Joseph, J. (2013). Resilience as embedded neoliberalism: a governmentality approach. *Resilience*, *1*(1), 38–52. doi:10.1080/21693293.2013.765741

Major, C., & Mölling, C. (2015). A Hybrid Security Policy for Europe. *SWP Comments*, (22). Retrieved from https://www.swp-berlin.org/fileadmin/contents/products/comments/2015C22_mjr_mlg.pdf

Manea, O. (2015). Hybrid War as a War on Governance. *Small Wars Journal*. Retrieved May 10, 2016, from http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance

McAslan, A. (2010, March 14). *The Concept of Resilience.Understanding its Origins, Meaning and Utility*. Torrens Resilience Institute, Adelaide, Australia.

Murray, W., & Mansoor, P. R. (2012). *Hybrid warfare: fighting complex opponents from the ancient world to the present*. New York: Cambridge University Press.

O'Malley, P. (2010). Resilient subjects: uncertainty, warfare and liberalism. *Economy and Society*, *39*(4), 488–509. doi:10.1080/03085147.2010.510681

Pospisil, J. (2013). Resilienz: Die Neukonfiguration von Sicherheitspolitik im Zeitalter von Risiko. *Austrian Journal of Political Science*, *42*(1), 18–42.

Ruiz Palmer, D. A. (2015). Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons. *Research Paper, Research Division - NATO Defense College, Rome* (120).

Siegert, J. (2016). Hybrider Krieg!? *Russland-Analysen*, (314), 21–24.