THE RĪGA CONFERENCE

Latvian Transatlantic Organisation

POLICY BRIEF

THE HYBRID CHALLENGE TO EURO-ATLANTIC SECURITY

Shota Gvineria

THE RĪGA CONFERENCE

POLICY BRIEF

2022

THE HYBRID CHALLENGE TO EURO-ATLANTIC SECURITY

Shota Gvineria

INTRODUCTION

One of the defining factors of the contemporary security environment is the quest for orienting among a wide array of modern security threats. In the 21st century, the Euro-Atlantic security community has been in search for the definition of the true nature of the crisis, conflict, and warfare. Almost every article on modern security terminology, including the ones cited in this paper, features the phrase – 'there is no universally applied definition.' As a result, the terms hybrid warfare, grey zone activities, asymmetric warfare, non-linear warfare, sub-threshold warfare, political warfare, information warfare, and cyberwarfare are defined by every security actor differently. This causes uncertainty and confusion among Western policymakers.

> **The West's lack of unified understanding has become an exploitable strategic vulnerability.**

Without a shared understanding of what modern warfare entails, there are limited possibilities for Western policymakers to come up with a joint and effective solution for countering underlying threats.

This paper argues that it will be much easier and less important to agree on universally accepted terms if the Western security community reaches a consensus on defining key features and operational aspects of the phenomenon of contemporary warfare. The overarching objective of the paper is to operationalize theories and modalities of modern warfare, decrease uncertainty and confusion surrounding existing conflicting concepts, and demystify perhaps the most controversial phenomenon – hybrid warfare.

Through analyzing Russia's example, the paper will apply the 'ends, ways, means' concept to explain how hybrid warfare strategies operate. The paper looks into whether the traditional national defense and security concepts or newer constructs such as resilience are applicable in the context of hybrid warfare. Further, the paper will illustrate how hybrid warfare strategies apply various instruments of national power and their correlation through the DIME (diplomatic, informational, military, economic) concept. Finally, outlining the role of cyberspace considerations in hybrid warfare is one of the aims of this paper.

THE CONTROVERSY OF HYBRIDITY-CONFLICTING TERMS, CONCEPTS, AND THEORETICAL FRAMEWORKS

In the aftermath of the illegal annexation of Crimea in 2014, hybrid warfare became ***the*** term to explain a combined use of various military and non-military instruments of national power for achieving political objectives. However, it has become common among Western security experts to denounce the term in recent years. Both components of the term, i.e., 'hybrid' and 'warfare', have been fiercely debated among Western academic and expert circles. Firstly, according to some experts, the contemporary security environment suggests that hybridity derives from the combined use of conventional and unconventional tools.[1] Others think hybridity indicates the mixture of conventional and irregular, predominantly kinetic and violent tactics. In this context, tools refer to the means employed, while tactics refer to the ways or 'how' contemporary wars are fought. The second controversy goes into more detail about the 'how' question. Based on the standard definition of warfare as the "modality of how to wage war," hybridity (as the new modality of modern-day warfare) is defined by some theories as "the integrated use of kinetic and non-kinetic tools." On the contrary, more military-centric theories argue that using the term 'warfare' can only be relevant when and if kinetic instruments of power

[1] Kennan, George, "George Kennan's 'Long Telegram'," February 22, 1946, History and Public Policy Program Digital Archive, National Archives and Records Administration, Department of State Records (Record Group 59), Central Decimal File, 1945-1949, 861.00/2-2246. Accessed October 04, 2021. https://digitalarchive.wilsoncenter.org/document/116178

are being employed for violent struggle.[2] Additionally, despite the cases of Russian military interventions in Georgia in 2008 and Ukraine since 2014 proving that conventional forces and armed conflicts could also be used as part of hybrid warfare strategy, many experts prefer using the term sub-threshold warfare (arguing that hybrid warfare fails to capture its own main essence: operating below the threshold of an armed conflict).

Most recently, an increasing number of experts and organizations have moved away from the term hybrid warfare and have chosen hybrid threats as the preferred term. NATO's vocabulary describes the phenomenon of hybrid threats as: "combining military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups, and use of regular forces." The European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) further describes the phenomenon as coordinated and synchronized action that targets democratic states' and institutions' systemic vulnerabilities through a wide range of means.[3] Hybrid CoE explains the difference between hybrid threats and hybrid warfare by relating threats to a broader phenomenon of combined use of military and non-military tools, while warfare refers to the application of those tools in particular theaters at particular points in time. While a differentiated approach towards threats and warfare is helpful from the theoretical perspective, it is still not essential in terms of finding solutions to the problem. The remaining question in this regard is what are we trying to deter, counter, or respond to - the threats or the warfare? This context drives these two different layers of hybridity towards the confusing practice of interchangeable use. To avoid confusion, this paper will rely on the term hybrid warfare to refer to the feature of the contemporary security environment that is described in the next chapter as the level of intensity of confrontation between the conditions of war and peace. Further, hybrid warfare strategy will be used to describe the ways employed by various actors for achieving political objectives using a combination of military and non-military instruments and tools. Finally, the specific

---

[2] Christopher S. Chivvis, "Understanding Russian" (RAND Corporation, March 22, 2017), https://www.rand.org/pubs/testimonies/CT468.html. Retrieved from: https://www.rand.org/pubs/testimonies/CT468.html.

[3] Giannopoulos, Georgios, "The Landscape of Hybrid Threats: A Conceptual Model." Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. 28 Feb. 2021. Accessed October 03, 2021. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model.

measure or a set of multiple measures implemented by the actors as part of their hybrid warfare strategies will be described as acts of hybrid warfare.

Notably, before 2014, only very few authors focused on hybrid warfare. One of the first definitions came from Frank G. Hoffman in 2007. He used the case of Hezbollah's strategy against Israel to describe hybrid warfare as employing multiple (predominantly kinetic) tactics simultaneously against an opponent.[4] Later, in 2018, he upgraded his definition and offered a nuanced comparison between different military-centric types of warfare, still heavily relying on the combination of kinetic and violent tools and tactics: "hybrid warfare simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, catastrophic terrorism, and criminal behavior in the battlespace to obtain desired political objectives."[5] In 2013, General Valery Gerasimov (Russia's Chief of the General Staff) published an article that gave a whole new impetus to the discussions on hybrid warfare, though with two significant differences. Firstly, in contrast to Hoffman, Gerasimov described a blend of political, economic, and military power to bear against adversaries that heavily focused on non-military instruments of national power as the key for waging contemporary warfare: "the role of non-military means of achieving political and strategic goals has grown, and, in many cases, exceeded the power of force of weapons in their effectiveness."[6] Secondly, Gerasimov didn't mention hybrid warfare even once and, instead of focusing on terms and definitions, explained his understanding of the modalities of "warfare typical for the 21st century" (типичная война XXI века) using the case of the Arab Spring as an example of the West using covert, non-military tools of subversion. Gerasimov's article gave an important boost to recognition of the political, cyber, and information instruments of national power in contemporary warfare.

---

[4] Hoffman, Frank G., "Conflict in the 21st Century". Potomac Institute for Policy Studies. Dec. 2007. Accessed October 02, 2021. https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[5] Hoffman, Frank G., "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *PRISM* | National Defense University, 8 Nov. 2018. https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges.

[6] Galeoti, Mark, "The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows*, 17 Sept. 2017. Accessed October 02, 2021. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war.

The term political warfare, which originated from George Kennan's long telegram sent to the state department from the US Embassy in Moscow in 1946, is perhaps one of the first ancestors of the term hybrid warfare.[7] The term is important as it emphasizes a key aspect of Soviet strategy – the employment of all the means at a nation's command, short of war – which in turn is the key in understanding contemporary hybrid warfare strategy. The most recent upgrade to the theory of political warfare has been further developed in US doctrine under the term grey-zone, which is characterized by: "intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."[8] Cyberspace, the information environment, and technology are often utilized to attack adversaries, causing harm comparable to actual warfare; however, those attacks are usually happening below the threshold of armed conflict. Cyberwarfare and information warfare are often mistakenly used interchangeably with other terms mentioned in this paragraph. **An important distinction is that cyber and informational environments are overarching domains for operation. At the same time**, **cyber and informational instruments and tools of national power are either enablers or multipliers of force in military or non-military domains rather than standalone warfare domains**. It is important to note that while cyber-attacks, as well as cyber-enabled information operations, can inflict limited kinetic consequences, they are still mainly tools of influence and interference rather than tools of warfare.

Another commonly used term, asymmetric warfare (defined as "war between belligerents whose relative military power differs significantly, or whose strategy or tactics differ significantly") eloquently accentuates one of the most important aspects of contemporary warfare: the importance of identifying and exploiting vulnerabilities of the adversary.[9] The term usually

---

[7] George Kennan. Telegram. The Charge in the Soviet Union (Kennan) to the Secretary of State. 22.02.1946. The National Security Archive, The George Washington University. Available at: https://nsarchive2.gwu.edu/coldwar/documents/episode-1/kennan.htm

[8] Joseph L. Votel, J., Cleveland, Ch., Connett, Ch., and Irwin, W., "Unconventional Warfare in the Gray Zone." *National Defense University Press*, 1 Jan. 2016. Accessed October 01, 2021. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/article/643108/unconventional-warfare-in-the-gray-zone.

[9] Lele, Ajey, "Asymmetric Warfare: A State vs Non-State Conflict." *Dialnet*, Facultad De Finanzas, Gobierno y Relaciones Internacionales De La Universidad Externado De Colombia, 30 July 2014. Accessed October 01, 2021. https://dialnet.unirioja.es/servlet/articulo?codigo=5134877.

refers to the situation when one side has an obvious dominance with conventional military capability, which gives incentive to their adversaries to think creatively and use asymmetric means for achieving objectives. Simply put, actors match their strengths against the vulnerabilities of the target.[10] Nonlinear warfare, in a fairly similar way, is fought when a state actor employs conventional and irregular military forces in conjunction with psychological, economic, political, and cyber assaults.[11]

The modern interconnected world has opened more and more possibilities for the practical application of various military and non-military tools of influence, interference, and warfare. Technological breakthroughs and the emergence of cyberspace have significantly multiplied the effectiveness and importance of the non-military instruments of power. The far-reaching effects of the toxic mix of those tools, combined with the possibility of staying below the threshold of armed conflict, if necessary, is what makes hybrid warfare a new phenomenon (even though hybrid strategies and tools have been part of almost all wars in the history of humankind). New generation warfare sums key features of contemporary warfare dispersed across various related definitions: "NGW seeks to bring about political or military outcomes without resorting to overt conventional military means, although the latter is not excluded."[12] The important limitation of all concepts and theories mentioned above is that none of them indicate where the threshold of conflict may be and what could be the criteria of defining an act of hybrid warfare VS an act of war. Some theories vaguely mention thresholds between acceptable and unacceptable consequences or tolerable and intolerable activities; however, in the absence of criteria, ad-hoc political decisions will have to be made to define whether each particular act of hybrid warfare was above or below the threshold of conflict.

The aim of this chapter is not to discuss the nuances of differences and

---

[10] "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *PRISM | National Defense University*, 8 Nov. 2018. Accessed October 01, 2021. https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges.

[11] Ball, Joshua, "What Is Hybrid Warfare? Non-Linear Combat in the 21st Century." *Global Security Review*, 10 June 2019. Accessed October 01, 2021. https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/.

[12] Derleth, James, "Russian New Generation Warfare Deterring and Winning at the Tactical Level." *Army University Press*, Sept.-Oct. 2020, Accessed October 02, 2021. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Derleth-New-Generation-War.

similarities related to all terms and definitions. However, it is essential to note that they primarily reside on the same core. The common denominator coded in all related terms is the combined use of conventional and non-conventional tactics on the one hand and synchronized utilization of military and non-military instruments of power on the other. These common denominators are an essential indicator for understanding the defining features and the real core of hybrid warfare. Therefore, instead of arguing about the differences and similarities of conflicting or interchangeable concepts, the **paramount objective of the following chapters of this paper will be to clarify the defining features of the contemporary security environment and the nuts and bolts of modern warfare hereinafter referred to as hybrid warfare**.

This paper suggests defining hybrid warfare as a coherent strategy of applying all elements of national power interchangeably or simultaneously to identify the vulnerabilities of the adversary and turn these vulnerabilities into pressure points.[13] The coherent strategy does not mean that all acts of hybrid warfare are interconnected and synchronized on the operational level. Instead, the coherent strategy emphasizes the continuity of the process in which adversaries constantly exploit each other's vulnerabilities and weaknesses. In this context, vulnerabilities can be defined as the opportunities that arise at different points in time to advance predetermined overarching objectives through waging hybrid warfare. Hybrid warfare may look chaotic because these random opportunities trigger seemingly unrelated cases of hybrid warfare in different shapes and in different contexts.

In other words,

> **coherent hybrid warfare strategy implies careful calculation of which tools would be more productive, relevant, and efficient based on the context in which specific hostile actions occur.**

[13] Gvineria, Shota, "Euro-Atlantic Security Before and After COVID-19", *Journal of Baltic Security*, 6, No. 1 (2020), 1–17 (2020). Accessed October 04, 2021. https://www.researchgate.net/profile/Shota-Gvineria/publication/347131164_Euro-Atlantic_security_before_and_after_COVID-19/links/5ff6bf54299bf1408878d002/Euro-Atlantic-security-before-and-after-COVID-19.pdf

Its indefinite continuity and opportunity-based application are the primary reasons why hybrid warfare is so challenging to detect, counter, or deter. For example, by being able to spot and quickly seize these opportunities, Russia has an advantage in utilizing hybrid warfare against the cautious and slow bureaucracies of democratic systems[14]. Many experts may argue that the definition presented above is too broad and might include anything that happens in contemporary security environments. Hybrid warfare should not become a simple way of classifying everything we don't like or understand. However, contrary to such critique, the definition highlights one of the main points this paper intends to make – hybrid warfare is a new normal. In the classical textbook sense, it may not qualify as warfare, but it is a new way of competition and achieving political objectives using all available tools.

THE SPECTRUM OF MODERN WARFARE

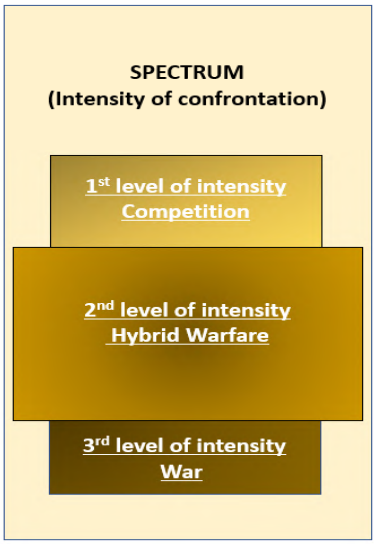

Figure 1: illustration of the three levels of intensity of confrontation

[14] The definition of hybrid warfare and corresponding explanation is provided in author's earlier work sited in endnote #16

According to the three stages in the spectrum of confrontation suggested in this paper in figure 1, the first level represents regular competition between actors, which is based on what traditional political theories qualify as peace. Most of the time, during the competition stage, actors rely on non-violent tools and act overtly within the framework of existing international rules and regulations. However, in today's uncertain world, where Euro-Atlantic security faces 360° of threats and challenges, it is difficult to relate the condition of absolute peace to the reality on the ground. The third level of intensity – war – is the most researched and regulated area of political and security studies. As the costliest way of achieving political objectives, war has always been a last resort. Military leaders (such as the aforementioned Gerasimov) have started to develop evolving strategies that adapt to new realities through the realization that there are more and more non-military tools that can supplement, reinforce, or even substitute military power. Actors launch conventional Wars and revert to overt violence only when the objectives and interests are inherently mutually exclusive and cannot be attained through other levels of intensity. Accordingly, in the 21st century, the necessity and the probability of conventional wars are limited. The shrinking of the traditional conditions for peace and war has opened more space for hybrid warfare – the second level of intensity. During this stage of confrontation, actors use a mix of non-violent and violent tools, rules and regulations are mostly ignored, and most operations happen covertly. These features of hybrid warfare are key for further unpacking its operational aspects.

In the 21st century, as evidenced through the analysis in previous chapter, the security environment has evolved and acquired some unprecedented characteristics. Western strategic thought, which is meant to inform defense and security strategy formulation among Western countries and institutions, is often blind to those new developments. To begin with, one of the most significant new characteristics of the contemporary security environment is the growing space between the conditions of war and peace. This phenomenon of so-called constant conflict is best reflected in the term unpeace – a situation that is described as lack of peace but not necessarily a war.[15]

[15] Merriam-Webster Dictionary, *Unpeace* (noun). Accessed October 01, 2021. https://www.merriam-webster.com/dictionary/unpeace.

However, based on traditional theories of political science and security studies, Western strategies and doctrines still recognize only two essential conditions – peace and war. This is one of the root causes of the confusing debate about the conflicting terms, concepts, and theories of contemporary warfare.

Another key characteristic, already extensively discussed in the previous chapters, is that states and non-state actors use a combination of military and non-military instruments of power to achieve political objectives. This second important aspect is associated with another limitation of Western strategic thinking, which derives from outdated understandings of war and warfare. Most Western doctrines recognize only two types of warfare – conventional and irregular. Conventional war is the chrestomathic, Clausewitzian approach toward warfare. Irregular warfare, as many of the other terms mentioned in this paper, contains some controversies. A classical definition of irregular warfare, as reflected in most Western doctrines, puts a strong emphasis on intra-state conflicts between states and non-state actors. On the contrary, David H. Uko's excellent analysis suggests that even state-based competition is likely to be "irregular" as various state actors are extensively using proxies or providing military support to non-state actors in other countries in order to indirectly promote their interests.[16] **The main problem with a limited and military centric outlook on contemporary warfare is that it hampers adequate incorporation of defense measures against non-military instruments into national defense and security strategies**.

To conclude, a central element for understanding hybrid warfare rests on its constantly continuous nature erasing the traditional boundaries between peace and war. There is no declared beginning or negotiated end to hybrid warfare. Based on this thesis, it is essential to acknowledge the fact that the contemporary spectrum of confrontation consists of three levels – peace, war, and hybrid warfare – the latter being the space in between the first two. Ironically, due to the complexity of the contemporary security environment, the seemingly most traditional and clear conditions of war and peace are most blurred. In other words, hybrid warfare has borrowed significant space from both peace and war, occupying most of the space among the three levels

[16] "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *PRISM | National Defense University*, 8 Nov. 2018. Accessed September 30, 2021. https://mwi.usma.edu/how-to-integrate-competition-and-irregular-warfare.

of intensity within the contemporary spectrum of confrontation, as suggested in Figure 1. Lack of acknowledgment of this reality is one of the main reasons why Western doctrines usually develop blind spots and fail to adequately define and respond to hybrid warfare.

THE NUTS & BOLTS OF HYBRID WARFARE

Simple analytical frameworks are often helpful in understanding the anatomy of comprehensive phenomena. To decompose the complexity of hybrid warfare and uncover the main operational aspects of hybrid warfare strategies, this paper will apply the basic 'ends, ways, means' construct. Another traditional framework DIME will be used to illustrate how various military and non-military instruments of power are applied for the execution of hybrid warfare acts.

ENDS

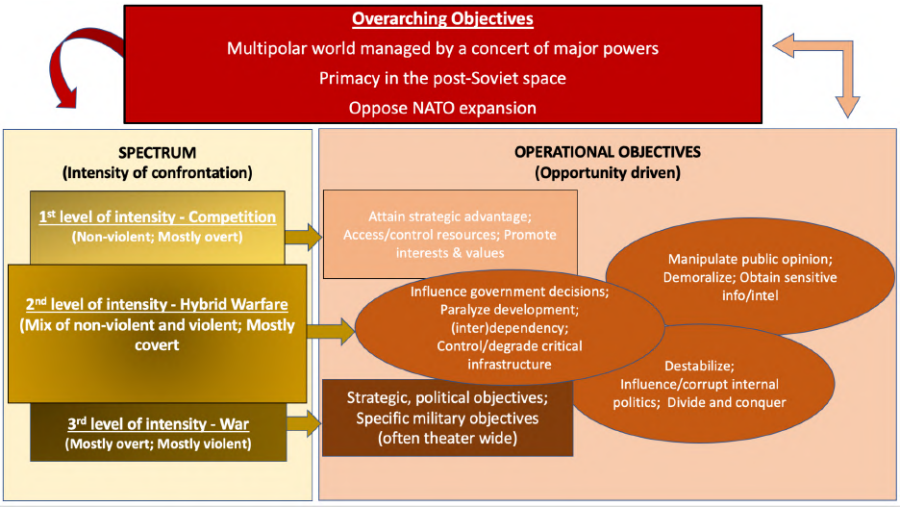

Figure 2: correlation between the level of intensity of confrontation, overarching objectives, and operational objectives (list of objectives in the figure is indicative rather than exhaustive)

Various actors have different objectives and different ways of achieving these objectives. In 2021, the expert group report commissioned by the NATO Secretary General clearly reflected that both revisionist powers Russia and China are increasingly posing hybrid threats to the Alliance.[17] It is important to analyze why revisionist powers such as China and Russia have chosen hybrid warfare as their preferred way of achieving political objectives. To attain asymmetric advantages, authoritarian regimes match their strengths (ability to make quick and reckless decisions, lack of transparency and accountability) with the vulnerabilities of the democratic system (slow decision making, lack of unity and resolve). Encouraged by cautious or even ambivalent Western approaches to countering hybrid threats, it has become obvious that authoritarian regimes have turned their ability to manipulate with the thresholds of conflict into a strategic advantage. Deniability of hybrid warfare acts and the difficulties in attributing these acts to specific actors is another incentive for the authoritarian affection for hybrid warfare. In other words, **authoritarian regimes revert to hybrid warfare knowing that hybrid warfare acts are very difficult to detect; thus, there is little probability of a resolute response while they operate below the threshold of armed conflict.**

The most visible match in Russian and Chinese hybrid strategies is the overarching objective of targeting rules-based systems with the aim of claiming freedom of action in their neighborhoods – spheres of exclusive influence. Other than that, Russia and China are very different actors and, accordingly, have their own ways and means of waging hybrid warfare. This paper will attempt to operationalize Russia's ends, ways, and means of waging hybrid warfare. Some universally applicable aims of Russia's hybrid strategy in all geographies at all levels of intensity of confrontation could be formulated as influencing public opinion and decision-making processes. Some of the operational objectives that are specific for the different levels of intensity of confrontation are presented in Figure 2.

The first important aspect to understand in Russia's hybrid warfare strategy is that survival of the regime is the first and foremost strategic objective

[17] NATO Defense College, "'NATO 2030. United for a New Era': A Digest." *NDC*, Brussels: NATO, 25 Nov. 2020. Accessed October 02, 2021. https://www.ndc.nato.int/news/news.php?icode=1509.

that guides all other dimensions of the strategy. National interests are often overshadowed by the mercantile interests of a regime, and acknowledgment of this fact helps avoid confusion and surprise every time the Kremlin makes irrational decisions. Second, another important point to keep in mind is that overarching objectives of hybrid warfare strategy often define the level of intensity of confrontation. Russia chooses whether to escalate or enhance partnership with other actors based on its understanding of interest and objectives in specific theaters at a specific point in time. Thus, overarching objectives define a spectrum of confrontation on one hand and shape operational objectives on the other. In turn, operational objectives directly contribute to achieving the overarching objectives, which makes hybrid warfare strategy a coherent cycle (see Figure 2).

More specifically, three overarching objectives that Russia is trying to achieve through waging hybrid warfare are reflected in Primakov's doctrinal ideas: Russia should strive toward a multipolar world managed by a concert of major powers that can counterbalance U.S. unilateral power; Russia should insist on its primacy in the post-Soviet space and lead integration in that region; and Russia should oppose NATO expansion at any cost.[18] The Kremlin perfectly understands that Russia does not have enough resources to fight for replacing the US as a superpower in a unipolar world, nor to challenge it in cold war type of confrontation. Therefore, Russia's primary goal is to strive towards a multipolar world where the great powers operate in their own spheres of influence. In Russia's understanding of a multipolar world, there should be no universally applicable rules, and big regional powers should have a legitimate right to advance their interests at the expense of their smaller and weaker neighbors without being criticized or challenged by external actors. In the meantime, Russia's hybrid strategy aims to reach foreign and security policy goals without the direct use of arms but through other levers of influence where possible.

---

[18] Rumer, Eugene, "The Primakov (Not Gerasimov) Doctrine in Action." *Carnegie Endowment for International Peace*, 5 June 2019. Accessed September 30, 2021. https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254?fbclid=IwAR1kzZCsajoxP8g04tmdgS986LYZmCLmiy50jQB9Jh-bQExY2EAFWEe_nuQ.

Russia choses its operational objectives per theater based on its assessment of the vulnerabilities of different adversaries.

> **Russia is consistently observing the vulnerabilities of different countries, which can open opportunities for planning and execution of hybrid warfare acts to advance specifically tailored objectives based on what the Kremlin can realistically afford in those countries.**

For example, in Ukraine and Georgia, Russia's objective is to extend influence through destabilization and thus keep those countries out of European and Euro-Atlantic institutions. In the countries that Russia does not directly see as part of its sphere of influence, for example Sweden and Finland, the objectives are less ambitious and escalatory and are guided by manipulation with public opinion to prevent those countries from joining NATO. Destabilizing those countries is riskier due to their EU membership, and their societal cohesion and defense systems are much less vulnerable than that of Ukraine's and Georgia's. Deriving from the revisionist objective of undermining the rules based international system, Russia's operational goals in large NATO member states (such as Germany, France, and Italy) are aimed at discrediting democratic values and systems and influencing internal politics through disinformation and corruption. The Baltic states have a unique place in Russia's hybrid warfare strategy. While Russia understands that the Baltic states are covered by NATO's article 5 security guarantee, its strategic thinking cannot accept the fact that the Baltics have escaped Russia's sphere of influence forever. Accordingly, Russia's hybrid warfare strategy aggressively aims at a complex combination of discrediting NATO, undermining the credibility of article 5, manipulating public opinion, weaponizing vulnerable minorities, and influencing internal politics.

WAYS

Hybrid warfare is a contemporary modality of confrontation and for waging warfare that implies integrated use of military and non-military instruments of power. Thus, from the strategic perspective, hybrid warfare in itself is a way of achieving political objectives, often without overt violence and direct use of military force. Gerasimov's famous article, which was initially labeled but later denounced as hybrid warfare doctrine, provides a perfect link between the definition provided above in this paper and Russia's actual hybrid warfare strategy.[19] What Gerasimov's article does in the first place is to cast light on his vision of the ways 'how' Russia should achieve the overarching objectives of its hybrid warfare strategy. Although he regards hybrid warfare as a western phenomenon, he still points out that in order to be successful countries (obviously including Russia) should "bring a blend of political, economic, and military power to bear against adversaries".

On operational level, ways of achieving objectives depend on the intensity of confrontation in which hybrid warfare acts occur and on the nature of the objective. For example the ways to destabilize certain countries or territories would include deployment of special operation forces and intelligence campaigns as well as infiltration of local political and social circles. However, for achieving the objective of manipulating with public opinion, the ways would focus on propaganda and disinformation campaigns, cyberspace operations and activation of local proxies. In Eastern Ukraine, the objectives of Russia's hybrid warfare strategy since 2014 includes both, destabilization, and manipulation with public opinion. Accordingly, the ways of achieving those interconnected objectives have been clustered under respective two lines of effort each leading towards specific desired outcomes. As hybrid warfare strategies get more complex with time, the ways of achieving multiple interconnected objectives are getting sophisticated and often range from military to non-military domains and cover full spectrum of instruments of national power.

---

[19] Galeotti, Mark, "The 'Gerasimov Doctrine' and Russian Non-Linear War". *In Moscow's Shadows.* 6 July 2014. Accessed October 03, 2021. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

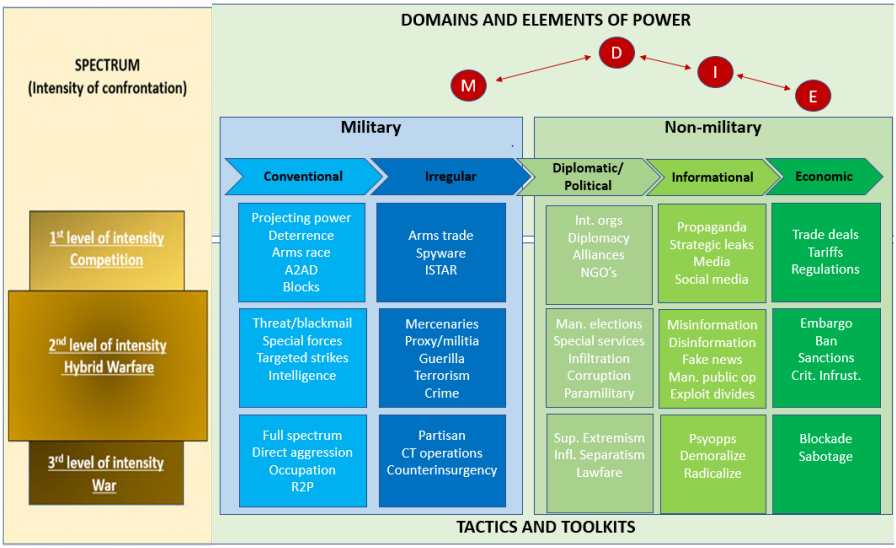

Figure 3: correlation between the spectrum of intensity of confrontation, military and non-military domains, instruments of national power and tools of influence, interference, and violence (list of tools in the figure is indicative rather than exhaustive)

To operationalize the concept of hybrid warfare, the key is to understand how military and non-military instruments of national power are applied interchangeably or simultaneously across the spectrum of confrontation. Figure 3 illustrates two domains – military and non-military – where instruments of national power could potentially be employed. Obviously, hybrid warfare strategies operate across both military and non-military domains. The military domain consists of conventional and irregular instruments of national power. In contrast, the non-military domain is more diverse and may contain many instruments of power. Many different models have been created to help better understand instruments of power, such as DIMEFIL (diplomatic, informational, military, economic, financial, law enforcement) and MPESII

(political, military, economic, social, information, infrastructure).[20] By applying the DIME concept and focusing on key non-military tools, Figure 3 also demonstrates that all instruments of national power are used not only to wage hybrid warfare but also across the whole spectrum of confrontation. The difference in involving all instruments of power across various levels of confrontation is that actors attempt to achieve different objectives by applying different tools on different levels. The figure also shows boxes with specific tools within each instrument of power. These tools, according to the level of intensity of confrontation, could be applied to achieve influence, interference, or violence. The difference between the boxes on various levels of intensity is that on the 1st level, both, military as well as non-military tools will be used but with the strong emphasis on non-military instruments aimed at exerting influence peacefully. On the 3rd level, again, both military and non-military tools will still be employed, but most of the emphasis will be on military tools aimed at kinetic and violent effects. The critique of the hybrid warfare term that argues that there is nothing new in the combined use of military and non-military instruments and tools might make sense from this perspective. However, what is new in the phenomenon of contemporary warfare is the growing scale, scope, and effectiveness of the non-military tools, especially on the 2nd level of intensity.

Russia's hybrid warfare strategy usually operates within the general modalities described in the paragraph above. **To understand the specific context related to Russia's typical application of means within hybrid warfare strategy, it is important to analyze the stakeholders and actors involved in the implementation of the strategy.** There are different types of actors that operate under various instruments of power, as illustrated in Figure 4. The purpose of this figure is not to provide a complete list of all actors but to illustrate that there are actual people who operate the instruments of power and to show a pattern of their interconnectedness.

[20] Johnson, Christopher, "Understanding National Power." *Chesterfield Strategy*. 4 Aug. 2019. Accessed October 03, 2021. https://chesterfieldstrategy.com/2019/08/04/understanding-national-power/.

The figure also shows the categories of different types of actors that form various instruments of power. For example, within the informational instrument, there are individuals involved from academia, government owned non-governmental organizations, controlled media, and social media. This instrument has its specific pattern of operation, but it is also inexplicably interconnected with other instruments. Interconnectedness reinforces effectiveness across all instruments. For example, the information instrument originates with overarching objectives and strategic narratives constructed by political leaders such as Primakov. Those narratives are then extended by ideologically driven academics such as Alexandr Dugin. At the next stage, strategic narratives are picked up and translated into specific geographical contexts by Margarita Simonian (manager at state-controlled media outlets RT and Sputnik). Finally, those fine-tuned messages are spread and multiplied by the organized bot nets and troll factories in order to reach as many hearts and minds as possible.

It is also important to note that most of the actors overlap across various instruments. A good example of this is the oligarch Jevgeni Prigozin, who is usually operating under the economic instrument of power but is heavily involved in the informational instrument as the owner of troll factories and in the military instrument as the creator of the infamous Wagner mercenary group. Moreover, under the political instrument of power,

> **agents of influence, infiltrated officials, and allied authoritarian regimes are also involved in promoting Russian narratives, including in Western countries.**

Figure 4: mapping of types of actors involved in implementation of Russia's hybrid warfare strategy and their interaction (list of actors in the figure is indicative rather than exhaustive)

Most of the people illustrated in the figure are involved in hybrid warfare acts that one way or another contribute to attaining the overarching objectives of Russia's hybrid warfare strategy. Synchronized operation across the instruments of power by the web of actors shown in the figure 4 constitutes the backbone of the coherent hybrid warfare strategy, even if not all the actors and their actions are always synchronized on the operational level.

THE ROLE OF CYBERSPACE CONSIDERATIONS IN HYBRID WARFARE

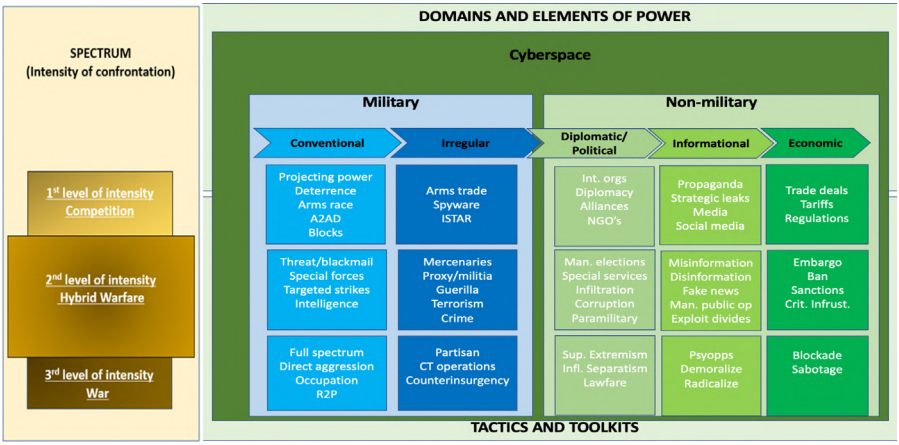

Figure 5: cyberspace as an overarching domain

To complete the mosaic of hybrid warfare strategy, it is important to fit in the key ingredient of the contemporary security environment – the cyberspace. Technological breakthrough and the emergence of cyberspace have triggered a monumental transformation of the contemporary security environment. As the defining factor of the modern security environment, cyberspace has acquired many important features. First, **cyberspace is an overarching domain that provides an operational environment for both military and non-military domains** (see Figure 5). Second, as a human-made environment, cyberspace itself is a technology, which is used to exploit and navigate all other traditional operational domains - land, sea, air, and space. Therefore, cyberspace has changed the ways of using instruments of power and tools across the board.

Several policy dilemmas turn cyberspace into the hybrid warfare battlefield for achieving revisionist objectives of authoritarian regimes. First, **there are no enforcement mechanisms to impose consequences for malign activ-**

ities in cyberspace. Moreover, there is even no universal understanding of rules and laws of responsible behavior in cyberspace. There has been some progress in synchronizing cyber policies and approaches within the EU and NATO formats such as Tallinn manual 2.0. However, on a global scale within the UN framework, there is still no agreed code of conduct to ensure that normative considerations can deter malicious activities.[21] Second, the issue of attributing cyber-attacks to the actors remains problematic. One of the main problems of attribution is that there are no clear footprints in cyberspace, and it is almost impossible to achieve full certainty about the operational details of various cyber-attacks. Traces of attacks are easy to wipe out and are even easy to manipulate with for leading investigation into the wrong direction. The lack of solid evidence related to cyber-attacks often makes attribution a political and strategic matter.

Most importantly, the **Western world is still divided on the concepts of approach to cybersecurity and on defining the proportionality of response to cyberattacks**. Some countries, such as Estonia for example, prefer a defensive approach to cyber operations and prioritize promotion of the applicability of international law in cyberspace.[22] In contrast, the US focuses on offensive cyber operations to project power and even takes pre-emptive actions whenever needed to neutralize potential threats in cyberspace. The so called defend forward approach of the US military, aiming to disrupt-and-degrade the capabilities of adversaries before they penetrate allied cyber defenses, is largely seen as escalatory by actors who practice a defensive approach.[23] The defending argument of the offensive approach claims that belligerent actors across the world are continuously trying to penetrate and influence Western systems and networks and that it is only a matter of time until any of those

---

[21] DigWatch, "UN GGE and OEWG." dig.watch. 2021. Accessed October 04, 2021. https://dig.watch/processes/un-gge.

[22] Ministry of Economic Affairs and Communications, "Cybersecurity Strategy: Republic of Estonia," 2019. Accessed October 04, 2021. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[23] U.S. Cyberspace Solarium Commission, "United States of America Cyberspace Solarium Commission Report," March 11, 2020. (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).

attacks will succeed. Furthermore, deniability of involvement has become a usual modus operandi for authoritarian regimes, which further complicates legal responses after an attack. It is obvious that the **lack of clarity on key policy considerations in the West emboldens Russia and other adversaries to utilize cyberspace for effectively challenging democratic system and advancing the overarching objectives of their hybrid strategies**.[24]

> **As information has clearly become a vital resource and source of power in the era of hybrid warfare, one of the most important features of cyberspace is its influence on the information ecosystem.**

Cyberspace has fundamentally changed the paradigm of navigating the information environment. Internet has enabled full digitalization of the ways to create, store, modify, exchange, and exploit information.[25] Authoritarian regimes effectively utilize cyberspace to manipulate opinions of internal and external audiences. Hordes of internet trolls and botnets – fake social media accounts creating and multiplying disinformation narratives – are deliberately targeting public opinion to sow discord, inflict divides, confuse societies, and obstruct democratic processes. Most importantly, cyberspace has underlined societal aspects of warfare. Individuals and groups of people become stakeholders in information warfare that results in the 'weaponization' of information. On one hand, societies and especially vulnerable groups of people have become a clear target for hybrid warfare. On the other hand, oligarchs,

---

[24] Paterson, T. & Hanley, L., 2020. Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. Australian Journal of International Affairs, March.

[25] Gvineria, Shota, "Euro-Atlantic Security Before and After COVID-19." Journal on Baltic Security, Volume 6, Issue 1. 1-17 (2020). Accessed October 04, 2021. https://www.researchgate.net/profile/Shota-Gvineria/publication/347131164_Euro-Atlantic_security_before_and_after_COVID-19/links/5ff6bf54299bf1408878d002/Euro-Atlantic-security-before-and-after-COVID-19.pdf.

strategic communications experts, media managers, and hackers often influence the hybrid battlefield more than armed combatants. Thus, high levels of confusion and uncertainty offered by the modern information environment, in combination with the vulnerabilities of cyberspace, provide vast opportunities for waging hybrid warfare. These are the most significant consequences of the emergence of cyberspace as the new battlefield.

In the modern world, critical infrastructure and essential services (such as healthcare, transportation, telecommunications, banking, quality of food, and many other vital processes that have a direct impact on the normal functioning of states) are inexplicably dependent on cyberspace. The kinetic effects of cyberspace are gradually increasing with the growing digitalization of vital processes and with more reliance on technological solutions, such as artificial intelligence and machine learning. Cyber effects have become more devastating, evolving from spying and DDoS attacks in the early days to doing severe physical damage to infrastructure and interference in elections. Thus, cybersecurity has emerged as one of the key aspects of national security considerations around the world. Increasing connectivity and reliance on information technology are vulnerabilities that are being exploited through cyberspace towards the ends of subversion of democratic systems, institutions, and societal cohesion. Cyber tools have become indispensable for extending malign foreign influences of the authoritarian regimes. Cyberspace is especially effectively used for influencing the decisions of various Western actors and manipulating with the public opinion within democratic societies. This feature defines cyberspace as the key enabler of hybrid warfare.

COMPREHENSIVE RESPONSE AND BUILDING RESILIENCE

Unexpectedly erupting modern security threats including cyber-attacks, disinformation campaigns, and other tools of hybrid warfare put unprecedented pressure on Euro-Atlantic security. As a result, the application of

traditional deterrence and defense concepts against highly unpredictable security threats and random challenges, which are less likely to be detected before they occur, is becoming increasingly difficult. Therefore, to cope with and recover from various adversities, increasing numbers of actors are searching for security solutions through the concept of resilience.

In its essence, resilience as a concept consists of three indispensable components.[26] The first component (successful opposition and resistance to external shocks) is related to resoluteness. The second defining feature of resilience is related to flexibility and the ability to recover and return to the former state after a shock or adversity. The third component is related to the capacity to adapt to new realities, which involves adjustment and compromise. Various studies have defined resilience in different ways, and scholars from various disciplines emphasize specific components of resilience based on the relevance to their own area of expertise.[27] However, researchers and experts from the defense and security sphere have not yet developed a comprehensive theoretical framework that would explain how to apply the concept of resilience to boost national and international security. This is an important gap in contemporary security studies.

The attempt of operationalizing the concept of resilience in defence and security context, originates from the idea of a comprehensive approach to security. Comprehensive security goes well beyond civil-military or interagency cooperation and entails cooperation between government, non-governmental organizations, and the private sector[28]. The inclusive process of involving multiple stakeholders from media, civil society, academia, and the expert community with the aim of achieving shared national security goals is sometimes referred to as an all-of-a-nation approach. What makes this approach essential is that most of the sectors of critical infrastructure

---

[26] Bourbeau, Philippe, *The Routledge Handbook of International Resilience*. (Routledge, 2016).

[27] Bourbeau, Philippe, "Resiliencism: premises and promises in securitisation research," *Resilience*, 1:1, 3-17(2013), DOI: 10.1080/21693293.2013.765738

[28] Rieker, Pernille, "From Territorial Defence to Comprehensive Security." Norwegian Institute of International Affairs. March 2002. Accessed October 04, 2021. https://www.files.ethz.ch/isn/27374/626.pdf.

in democracies (such as the energy, transportation, banking, and medical sectors) are owned and governed by private companies. Thus, for the comprehensive approach to be effective, political leadership should coordinate common national security objectives across all sectors and facilitate collaboration to achieve those objectives.

In most countries, the National Security Council or Prime Minister's Office is responsible for coordination on political and strategic level. State agencies develop contingency plans for their involvement in various crises and receive specific ad-hoc instructions based on their role in countering hybrid threats. Armed forces have a limited role in the operational aspects of countering hybrid warfare. It is crucial to make sure that what different stakeholders do under their spheres of competence does not contradict but reinforces one another. On the international level, organizations such as NATO and the EU are trying to coordinate what different member states are doing nationally to counter hybrid threats. While NATO and the EU have some institutional capabilities for countering a few specific aspects of hybrid warfare, the main capabilities (and therefore responsibilities) for applying comprehensive security measures remain with member states. One of the main difficulties in successfully adopting a comprehensive approach is the huge gap in how political and military leaders understand all aspects of contemporary warfare. The difference in military and civilian perceptions of hybrid warfare is well reflected in the debate about various conflicting definitions presented in previous chapters of this paper. Therefore, **the key to an effective response to hybrid warfare strategies is cooperation and coordination across all state agencies, critical sectors, and international alliances**.

There is a detailed definition specifically related to the national security context of resilience provided by the British doctrine: "ability of the community, services, areas or infrastructure to detect, prevent, and, if necessary, to withstand, handle and recover from disruptive challenges".[29] NATO, as a

[29] Cabinet Office, UK Civil Protection Lexicon Version 2.1.1.

multinational security organization, defines resilience in the following way: "resilience is a society's ability to resist and recover easily and quickly from shocks and combines both civil preparedness and military capacity".[30] Doctrinal definitions by other actors also clearly underline that strengthening resilience is related to effective application of both military and non-military elements of national power. Among the complicated and multilayered definitions developed by states and international organizations, there are a few phrases commonly used during expert discussions when attempting to explain the notion of resilience: the immune system of a nation, fixing the roof in the sunshine, prepare for something that might never happen.[31] The term alludes to the necessity to prepare for unknown threats and is basically used as the buzzword to emphasize a comprehensive approach to security. At this point, there is no evidence that the concept of resilience has been successfully applied as a defense and security concept. This, in turn, augments the problem of finding reliable solutions against sophisticated hybrid warfare strategies of authoritarian adversaries.

According to the analysis provided in this paper, **the main features of the contemporary security environment are that the boundaries between conventional and unconventional forms of conflict are blurred and that application of non-military instruments of national power by a multiplicity of state and non-state actors is considered as a new normal**. Addressing the wide range of hybrid warfare strategies directed against Western states and institutions requires acknowledgement of the urgency and indispensability of including all relevant stakeholders and all instruments of national power in coordinated and synchronized national defence processes. The main message of this paper is that **defense against not only conventional military but also non-military and cyber threats should be adequately incorporated in the national security planning and strategy formulation**

[30] North Atlantic Treaty Organization. (2020). Resilience and article 3

[31] Canal, Bonnie, *Preparedness vs. Resilience, Are They the Same Thing?* 02 Oct. 2015. Accessed October 03, 2021. https://www.linkedin.com/pulse/preparedness-vs-resilience-same-thing-bonnie-canal/.

processes of the Western countries and organizations. Most importantly, it is vitally important that the key Euro-Atlantic security actors genuinely understand hybrid warfare and engage in a coordinated efforts to push back authoritarian aggressive policies aimed at undermining the rules based international system, democratic societies, systems, and values.

THE LATVIAN TRANSATLANTIC ORGANISATION (LATO) IN ACTION

LATO

LATO is a non-governmental organisation established in 2000. Its aims are to inform the public about NATO and Latvia`s membership in the Alliance, to organise informative public events about Latvian and Euro-Atlantic security issues, to promote partnerships with other countries, to lay the foundations for Latvia`s international role as a member of NATO, and to foster the international community's understanding of Latvia`s foreign and security policy aims. During the past 20 years, LATO has numerous achievements to be proud of. LATO organises the most influential security conference in the Baltic Sea region: The Rīga Conference facilitates discussion about issues affecting the trans-atlantic community and annually gathers international experts in foreign affairs and security/defence matters, policy makers, journalists, and business representatives. LATO promotes policy relevant research on topics such as gender equality, peace and security, resilience in the borderland, and the subjective perception of security. A series of various initiatives intended for increasing the interest of Latvian, Baltic and European youth in security related issues hav been put in motion, including an annual future leader's forum and masterclasses for young political leaders. LATO's most recent project is the Secure Baltics platform, which serves as an information hub for those who are eager to join the debate on international security.

CONTACTS:

E-mail: lato@lato.lv

phone: (+371) 26868668

Facebook: Latvian Transatlantic Organisation

Instagram: lato_lv

Twitter: @LATO_L

SECURE BALTICS

LATO has launched a new internet platform SecureBaltics (www.securebaltics.eu). The site gathers different materials – policy briefs, discussions, interviews, studies, educational materials – created in the framework of the Rīga Conference, as well as work from our partners. It is a stable platform that the Rīga Conference community can rely on and use as a credible source of information in the region.

Purpose

The purpose of the platform is to collect the know-how that is generated by the excellent minds gathered at the Rīga Conference on an annual basis. The Rīga Conference gathers regional and international experts in foreign policy and defence, academics, journalists, and business representatives by promoting the discussions on issues affecting the transatlantic community. It has been growing in influence since its inception in 2006.

Every year, for two days the National Library of Latvia is the centre of the most important regional discussions on security issues. However, it is not enough to engage in these discussions only once a year. Therefore, LATO developed SecureBatlics as a practical tool which can encourage the use of any resources and materials that have been produced as part of the Rīga Conference or its follow-up events.

Reach

The platform tries to provide materials in both, English and Latvian, in order to reach multiple audiences. It is intended for the traditional Rīga Conference community of opinion leaders and experts in foreign policy and defence matters as well as any other interested parties that could benefit from the generated materials such as high school teachers looking for study materials.

Vision

LATO hopes that SecureBaltics will become the go-to hub for resource associated with defence and security issues in the Baltics within the next few years.

Materials

The platform SecureBaltics provides resources:

- For all interested parties, including expert community, in the form of interviews, policy briefs, commentaries on topical issues
- For teachers and lecturers in the form of study materials and tests that can be included in academic curriculum
- For students in the form of lectures and study materials, as well as interactive study materials through games.

Partners

The SecureBaltics portal is supported by the Ministry of Foreign Affairs of the Republic of Latvia and the Ministry of Defence of the Republic of Latvia.

Editor: Žaneta Ozoliņa
Project manager: Sigita Struberga
English language editor: Katrīna Baltmane
Cover design: Laura Benga
Layout: Inese Siliniece

Publishing house: SIA GREEN PRINT
17 Andrejostas street 17, Riga, LV-1045

ISSN 2661-5789

ABOUT THE AUTHOR

Amb. Shota Gvineria joined the Baltic Defence College as the lecturer in Defence and Cyber Studies in July of 2019. He is also a non-resident fellow at the Economic Policy Research Center since 2017. Earlier, Amb. Gvineria has been working on various positions in Georgia's public sector. Among other positions, Shota Gvineria served as the Deputy Secretary at the National Security Council of Georgia. He covered NATO's integration and security policy related issues as the Ambassador at Large in the Ministry of Foreign Affairs of Georgia. In his previous capacity until August 2016, he held the position of the Foreign Policy Advisor to the Minister of Defense of Georgia. Through 2010-14, he served as the Ambassador of Georgia to the Kingdom of the Netherlands. In 2010, Amb. Gvineria was promoted to the position of a Director of European Affairs Department at the Ministry of Foreign Affairs of Georgia. Prior to that, in he served as a Head of NATO Division at the Ministry of Foreign Affairs of Georgia. In the period from April 2006 until October 2008, Shota Gvineria was posted as the Counselor of the Georgian Mission to NATO. Amb. Gvineria holds MA in Strategic Security Studies from Washington's National Defense University. He also earned his MA in International Relations from the Diplomatic School of Madrid and Public Administration from the Georgian Technical University.

Ministry of Foreign Affairs Republic of Latvia

Ministry of Defence Republic of Latvia

LATO LATVIAN TRANSATLANTIC ORGANISATION

NATO OTAN