NATO

AND THE FUTURE OF PEACE IN EUROPE:

TOWARDS A TAILORED APPROACH

Editor: Marcin Terlikowski
Authors: Artur Kacprzyk, Kacper Rękawek, Witold Rodkiewicz, Andrzej Wilk

PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NATO and the Future of Peace in Europe: Towards a Tailored Approach

Editor: Marcin Terlikowski

Authors: Artur Kacprzyk, Kacper Rękawek, Witold Rodkiewicz, Andrzej Wilk

Warsaw, 2016

This report is the result of a series of expert meetings initiated by the Department of Foreign Policy Strategy of the Ministry of Foreign Affairs of the Republic of Poland in cooperation with the Polish Institute of International Affairs (PISM) and the Centre for Eastern Studies (OSW).

Editor
Brien Barnett

Technical editor and cover design
Dorota Dołęgowska

Cover photo
Nicolas Raymond, www.shutterstock.com

ISBN 978-83-64895-79-1 (pb)
ISBN 978-83-64895-80-7 (pdf)

Polski Instytut Spraw Międzynarodowych
ul. Warecka 1a, 00-950 Warszawa
phone (+48) 22 556 80 00, fax (+48) 22 556 80 99
pism@pism.pl, www.pism.pl

Contents

Executive Summary

- The European security environment is undergoing a structural change due to rapid evolution and an increase in interdependencies within an entire set of threats; NATO cannot respond to all of them because of natural limitations, so instead it should rely on a tailored approach that would build on the Alliance's comparative advantages to tackle these challenges, either as the main vehicle or an enabler of other organisations or formats.
- The threat from Russia is persistent and strategic, and boils down to its revisionist approach to the entire post-Cold War political and legal order in Europe; in pursuit of this goal, Russia is ready to use military tools, particularly against NATO's Eastern Flank, where it can rely on its overwhelming military potential and anti-area/access denial (A2/AD) capabilities.
- In response to the Russian threat, NATO should launch a more comprehensive adaptation of its deterrence and defence policy and capabilities; first and foremost, the Alliance should change its conventional posture on the Eastern Flank by balancing its ability for reinforcement with a multinational forward presence of sufficiently large combat forces and proper military infrastructure in the region.
- NATO also needs to respond to the Russian non-conventional threat, which includes both aggressive nuclear signalling and hybrid warfare while relying on civilian or paramilitary proxies; to this end, NATO should move towards updating its nuclear policy and, at the same time, develop cooperation with the European Union in detecting and reacting to potential hybrid-type crises.
- A specific task for NATO is to properly address the looming threat of cybersabotage, which may be part of a hybrid conflict scenario or materialise on its own; in any case, the potential that cybersabotage could result in large material losses and high casualties calls for NATO to acknowledge cyberspace as a new domain for warfare and adopt a "cyberdefence pledge" aimed at developing the proper capabilities among the Allies and making them available for collective action.
- Asymmetric and non-military threats—terrorism, cyberattacks, mass migration, international organised crime—have neither the potential nor the aim to endanger the sovereignty or territorial integrity of European states; nevertheless, their long-term effects may include disruption of socio-economic life and weakening of the governance structure, and therefore they should be addressed immediately and in a skilled manner.
- In response to terrorism, cyberattacks, mass migration or international organised crime, NATO should seek out the role of enabler of member state or partner responses, offering its unique capabilities and experience to other organisations or formats that may be better suited to solve multi-dimensional crises that involve not only security-related issues; unleashing the full potential of the EU–NATO strategic partnership would be instrumental in this regard.
- To further stabilise the transatlantic area, NATO should rethink its partnership system to one that should deliver more with regard to the Alliance's task of building cooperative security; reinforcing the stability of Ukraine and Georgia through further military cooperation programmes and strengthening their resilience is a crucial task in this regard, but NATO should also further develop non-European partnerships, e.g., with Jordan, and continue to reinforce cooperation with Finland and Sweden, which play a pivotal role in security of the Baltic Sea region and the entire Eastern Flank.

Introduction

"NATO exists for peace by collective security". This quote by Lord Ismay, the first Secretary General of NATO, encapsulates the central purpose of the Alliance, which has been directly tasked with preserving the peace in Europe for over 60 years, longer than any other organisation on the continent. Hence, today's considerations on the future of NATO, its policies and capabilities, are in fact tantamount to deliberations on the future of European peace and on how to maintain it. At the same time, answers to pressing threats and challenges are urgently sought, as the European security environment is undergoing a structural change.

This transformation is primarily characterised by rapid developments and significant interconnections between multiple threats of a military, asymmetric and non-military nature. After Russia forcibly annexed Crimea and then intervened militarily in eastern Ukraine, military aggression, considered a remote threat for the last two decades, is back on the European security landscape. In the strategic vicinity of Europe, non-state actors driven by radical ideology, particularly the so-called Islamic State in Iraq and Syria (ISIS) and Al-Qaeda, have conquered large amounts of territory and established quasi-states, which enabled them to inspire or directly control terrorist networks in Europe, North Africa and the Sahel. Attacks such as those in Paris, Brussels or Bamako testify to their growing capabilities. The collapse of the state in Libya and Syria, both torn apart by internal and yet highly internationalised conflicts, generated mass migration that spilt over to Europe and put a strain on both the EU's common migration policy and European solidarity. In cyberspace, disinformation, sabotage and espionage attempts number hundreds of thousands a day. On top of these threats, the post-Cold War political and legal order has been challenged by Russia, which, through its military posturing, puts pressure on the West in order to revise the international regime in a way that would compromise the sovereignty of individual states.

To date, European security institutions have been largely unable to deliver a comprehensive and coordinated response to this "Gordian knot." Yet, the North Atlantic Alliance seems to have responded swiftly and substantially. In a move to reinforce the security of its member states in Central and Eastern Europe, which face a growing threat from Russia, NATO has launched a number of reassurance measures. In response to the mass migration across the Mediterranean, NATO took several steps, including a maritime monitoring operation in the Aegean Sea. The Alliance also has been developing a cyberdefence policy and tools to address new methods of coercion, subversion and aggression that combine a wide array of military and non-military instruments and now referred to as "hybrid warfare."

The history of NATO is one of continuous adaptation to keep up with evolving threats. The Alliance is now expected to offer its member states a comprehensive toolkit to address the deterioration of the security environment in Europe. While reaching consent on the Alliance's further adaptation may be difficult given the obvious differences in threat perceptions and security priorities among the Allies, the unity of NATO can be preserved if the debate is driven by the principle of following a tailored approach. This could be understood as a rule, meaning that whenever the Alliance can bring to bear genuine added value when addressing a given threat, it should be the primary, although not the only, responder. If the political-military nature of NATO makes it hard to deliver a counter to some other types of threats, mainly asymmetric or non-military, the Alliance should look for niches where it can act to enable or support other organisations or coalitions. This kind of thinking is, of course, not new to NATO but has been somewhat lost from the debate in recent years, as the Alliance has been trying to respond to imminent and poorly understood threats of an asymmetric or non-military character and doing so in a poorly coordinated manner. Meanwhile, only a tailored approach, in which NATO chooses whether to enable other partners or take leadership with regards to a given threat or in a given theatre, can help Europe effectively address the increasing and intertwined set of threats it faces.

This report is the result of a series of expert meetings initiated by the Department of Foreign Policy Strategy of the Ministry of Foreign Affairs of the Republic of Poland in cooperation with the Polish Institute of International Affairs (PISM) and the Centre for Eastern Studies (OSW), the two largest public policy research institutes in Poland. Related seminars took place in the selected capitals of NATO member states and partners between autumn 2015 and spring 2016 and focused on the situation on NATO's Eastern Flank, while also taking into the account other aspects of the Alliance's need for adaptation in a changed European security environment. This report, however, is not a strict record of the discussions from these seminars and instead builds on their main themes, findings and conclusions. This is also the reason for the difference in the depth and breadth of the issues. The report is split into two parts: the first contains an analysis of threats to the security of Europe, selected on the basis of relevance to NATO, followed by a proposed Alliance response to each; in the second part, recommendations are made in line with the tailored-approach principle as proposed and defined above.

I. Revisionist Russia

Russia poses a threat both to NATO and to European security because it is pursuing policies aimed at a fundamental revision of the post-Cold War order in Europe, using methods and instruments that are contrary to international law and to the principles of the OSCE. This revisionist thrust of Russian policy is rooted in the refusal of the country's ruling elite and large sections of its society to accept the political and security order that emerged in Europe in the wake of the collapse of the Soviet Union in the late 1980s and 1990s. In its efforts to undermine and revise this order, the Kremlin is pursuing its own vision of a European security order. It seeks to provide for the peculiar security needs of the Kremlin by making the security of Central and Northern European countries (members of NATO and/or the EU) dependent on Russia, as well as restricting the sovereignty of the post-Soviet states.

The Kremlin's revisionist vision consists of three elements that can also be seen as strategic objectives pursued by the Russian government: 1) an exclusive sphere of influence over the post-Soviet countries; 2) a strategic-military buffer zone in Central and Eastern Europe encompassing the former Warsaw Pact countries; 3) a "concert of great powers" arrangement tantamount to a Russian "co-decision" zone in Europe (including Western and Northern Europe, the Balkans and the Mediterranean).

These three objectives are being pursued by the Kremlin in the context of a broader, anti-American agenda. This agenda is designed to reshape the global international order in the direction of a global oligarchy of great powers, based on the reaffirmation of the traditional Westphalian principle of absolute national sovereignty for the great powers, while granting them the role of "regional policemen" in their immediate neighbourhoods.

Under its current leadership, Russia has pursued a consistent policy of constructing its own sphere of influence in the post-Soviet area by employing a wide variety of methods, including support for political separatism, instrumentalisation of ethnic conflict, political subversion, economic pressure, and last but not least, direct military aggression. The ultimate objective is to create a Russian-dominated economic and security bloc composed of countries with de facto limited sovereignty, whose foreign, defence and even domestic policies would be subject to a Russian veto (enforced, as in the cases of Georgia and Ukraine, by the direct use of force). Their economies would be ultimately subordinated to institutions dominated by Moscow (such as the Eurasian Economic Union).

The Russian leadership has been consistently opposed to all and any efforts undertaken by the former Warsaw Pact states to ensure their security through integration with Western security structures. It has protested and threatened to retaliate (including with nuclear strikes), first against NATO enlargement and later against the planned enhancement of the military capabilities of NATO members in the Baltic and Central European region, and in particular against the installation in the region of U.S. military facilities. The logic implicit in Russian proposals for providing security for Central Europe (such as the joint security guarantees by Russia and NATO, the 1995 OSCE-based pan-European collective security arrangement, the 2008 proposals by then-President Dmitry Medvedev for the European Security Treaty, and the Russian position during the negotiations over adjustments to the CFE Treaty in the 1990s) suggests that Moscow is aiming to turn the region into a de facto military buffer zone, while Russia would enjoy a structural military preponderance in the border area.

Beyond Central Europe, the Kremlin has pursued a policy designed to transform Western Europe into a militarily and politically powerless area that would serve as Russia's strategic backyard, providing it with economic opportunities, capital and technological resources for its own neo-imperial integration projects in the post-Soviet area, as well as maintaining its status

as a globally influential great power in the context of a multipolar international system. To achieve those aims, the Kremlin has worked to drive a wedge between Europe and the United States, undermine and paralyse NATO as the collective defence mechanism of the Euro-Atlantic community, and to subvert and weaken the European Union. In pursuit of these objectives, the Kremlin's policy has moved over the last few years to qualitatively new ground through its attempts to influence the internal politics of key West European states by means of propaganda and providing support to some anti-establishment political forces. Ultimately, Moscow's objective seems to be an arrangement reminiscent of the 19th century "concert of great powers" with the main continental European powers.

The threat from Russia is even greater because in pursuing these objectives, the Kremlin is acting according to a strategic culture based on a Darwinian vision of international relations, the essence of which is a struggle for survival between rival great powers. This culture is characterised by an extreme suspicion of outsiders and a conspiratorial view of the world. As a result, the Kremlin leadership is inured to using violent and subversive means to achieve political results and treats political and economic competition as a form of warfare.

To advance the aforementioned strategic goals, the Kremlin, especially in recent years, has turned increasingly to military instruments that are hostile towards NATO, the EU and their member states.

The war in Georgia in 2008, together with the failure of Russian proposals to redraw the European security architecture system, led to an increase in Russia's efforts to strengthen its real military potential in Europe, and also—with the aggression against Ukraine that started in 2014—to an open confrontation with NATO in the post-Soviet area. Russia's activities related to this can be divided into four groups: 1. the priority given to modernising and increasing its military capability in the European part of Russia; 2. the creation in the western areas of Russia and Belarus of a defence and monitoring system blocking NATO forces' free access to the area of potential operations in member states on the Alliance's Eastern Flank (A2/AD); 3. the intensification of training activities aimed at preparing the Russian Federation's armed forces for clashes with NATO forces; 4. information warfare and psychological operations.

After the reorganisation of the Russian Federation's armed forces (starting in 2012) was completed (the transition from the post-Soviet structure of a mass army based on a general draft to one with a high degree of professionalisation and considerable mobility), the focus was switched to increasing the military potential in the European part of Russia, primarily in the Western Military District, which directly borders the member states of NATO. In the westerly strategic direction (from the Russian perspective), which had until then been the only such vector, divisional structures were created, by developing them on the basis of existing brigades (such as the elite 2nd Mechanised Division and 4th Armoured Division, stationed in the vicinity of Moscow), as well as forming new ones from scratch (three mechanised divisions, located directly on Russia's western border, whose formation will be completed before the end of 2016). Taken together with the creation in 2015 in the Western Military District of a new operational-level headquarters, the 1st Armoured Forces, this clearly indicates that Russia is building up military capability of a purely offensive nature directed at the West. Armed units in the Western Military District are being given top priority, in the processes of both technical modernisation (they will be the first to receive serial models of new tanks and armoured vehicles in 2016–2017), and of professionalisation (in 2017, professional and contract soldiers are to make up about 80% of the total military personnel of the Russian Federation's armed forces).

The current integration of Belarus into the Russian air and missile defence system, and the creation on the western borders of Russia and Belarus of an integrated electronic reconnaissance and combat system, has led to the creation in the northern section of NATO's Eastern Flank (i.e., the three Baltic States and a part of Polish territory) of a situation which is very unfavourable to

any military actions NATO may take, bringing them to the level of what in American military terminology is referred to as "anti-access/area denial" (A2/AD). In addition to the aforementioned integration of the Belarusian component into the Russian systems, the creation of the A2/AD setup was enabled by a new generation of units that could impact military activity in the Baltic States and Poland (primarily the S-300 and S-400 air and missile defence systems, and a new generation of radar stations and electronic warfare systems) from their permanent locations in Russia and Belarus. The A2/AD capabilities of both countries are further enhanced by the potential of their land forces, combined with the geography of the region (including the relatively narrow land connection—known as the Suwałki Gap—between the Baltic States and the rest of the NATO area). It stretches from Kaliningrad Oblast to the border with Belarus and is located entirely within the range of fire of artillery brigades located there. The whole of Estonia and Latvia are also within reach of Iskander ballistic missiles (500 km) from the 26th Missile Brigade. After the 152nd Missile Brigade was relocated to the town of Chernyakhovsk in Kaliningrad Oblast, its Iskander missiles can also reach Lithuania and almost the entire territory of the Republic of Poland (the Tochka rockets that have been stationed there up to now have a range of 120 km).

The occupation of Crimea has allowed Russia to establish an A2/AD zone in the southern sector of NATO's Eastern Flank, although as yet it does not cover the territory of any NATO member states. It does cover southern and eastern Ukraine, as well as the central part of the Black Sea basin. Parts of the territories of Bulgaria, Romania and Turkey are within range of reconnaissance systems located in Crimea. The Black Sea A2/AD area could only be extended after the introduction of the next generation of S-500 air and missile defence systems (and from the offensive perspective, Iskander missiles); at this point, however, there are not even any S-400 systems present in Crimea.

The westerly exercises of the Russian Federation's armed forces—especially *Zapad* (West) and Shchyt Soyuza (Union Shield), conducted together with Belarus, and the *Ladoga* exercise conducted by Russia's Air Forces—indicate the systematic preparation of troops in the Western Military District for action in the area of NATO's Eastern Flank. The main elements of these exercises include quick deployment of forces from the depths of Russia to airports and military areas in Belarus and/or Kaliningrad Oblast (via air and rail transport), as well as the creation of transport and communications networks several hundred kilometres in size, and the deployment of field hospitals (in these exercises, it is logistical formations and not combat formations that are most heavily used). In the strategic exercises (on an all-Russian level), it is worth noting the use as a second strategic wave of units from the Central Military District, which have been transferred to the European part of Russia from beyond the Urals. From previous exercises, it appears that the process of relocation and combat readiness at the new locations will take from 24–48 hours (for Air Force and Airborne Troops formations) up to one week (Army formations).

In Russia's information war against NATO, both actual military activity as indicated above and classic disinformation tactics are used, such as leaks to the media (including directly to Western media) about the deployment of missiles with nuclear warheads in Kaliningrad Oblast (which does not preclude the possibility that, in reality, tactical nuclear munitions have been present in that area since the Cold War), or exercises of nuclear attacks on targets in Poland and the Baltic States. Periodic reports about the deployment of Iskander missiles in Kaliningrad Oblast should be treated similarly; according to schedule, they will most likely be deployed there by the end of 2018, and will coincide with the activation in Poland of one element of the U.S. Ballistic Missile Defence System, constituting an American contribution to NATO Ballistic Missile Defence Capability (when that happens, Russia will present the deployment of its missiles as a response to "aggressive" U.S. policy). These measures are aimed first and foremost at distressing the public in the West, especially in combination with a parallel message that the potential risk does not include those countries of Western Europe that are ready to accept the demands of Russia, but only those states on NATO's Eastern Flank, which Russian propaganda describes as politically

subservient to the United States. Another element of direct psychological pressure, not only on the public but also on NATO troops, is the increasingly frequent incidents between planes and ships of Russia and NATO. For many years, these have been limited to violations of airspace; however, from 2014 (initially in the waters of the Black Sea, and presently mainly in the Baltic region), Russia has increasingly been simulating attacks on NATO units or carrying out dangerous manoeuvres (risk of collisions).

II. The Asymmetric and Non-Military Threats in Europe's Neighbourhood

Asymmetric and non-military threats, rapidly evolving in Europe's immediate neighbourhood, as well as in Europe itself, are widely considered as compelling as the threat posed by Russia. Yet, their nature is utterly different and they cannot be perceived as being strategic *per se*. Terrorism, cyberattacks, organised crime and mass migration put a huge strain on the resilience of individual states and international organisations. But for European countries, these threats have neither the critical mass nor an aim of questioning a state's territorial integrity and sovereignty. The long-term effects of these threats are likely to include disruption of the functioning of state structures, economy and society, but not the existence of the European states themselves nor their sovereign right to choose their alliances and other, both internal and external, policies. In a particular sense, terrorism and crime could not have existed without the state, which they exploit in pursuit of their goals, but do not intend to destroy. This, however, does not mean that they are not a priority challenge for European security. Precisely for the reason that they come in a set of entangled and interdependent threats, they need to be addressed swiftly and with optimal tools. If not addressed, they may, first, further complicate and grow, and, second, gradually undermine European political solidarity, which is already being put under immense pressure.

The threat of international Islamist terrorism is widely considered to be as urgent—even if not as strategic, in the sense of not threatening the entire political and legal system in Europe—as that posed by Russia. The deadly attacks in Paris in November 2015 and in Brussels in March 2016, organised and carried out by networks of radicals who had fought in Syria and then returned with a task to establish terrorist cells, have put the focus on the deeper source of the threat. NATO now borders two quasi-state entities: the "caliphate" declared by the Islamic State in Iraq and Syria and Al-Qaeda's emerging "emirate" in northwestern Syria. These entities will continue their reliance on terrorism as the weapon of choice against what they broadly understand as the West, and further, given the right circumstances and opportunities, could subsequently gravitate towards other means of waging warfare.

For the foreseeable future, Europe will continue to face an elevated jihadist terrorism threat, which first manifested itself in France as early as in 1995 in the Paris Metro and RER bombings (staged by the Armed Islamic Group, or GIA, an Algerian Islamist terrorist organisation). One would expect that the continent should be well prepared to address this threat. After all, Western Europe suffered about 15,000 terrorist attacks between 1970 and 2014. For the first time, however, Europe is faced with the threat of a series of mass-casualty attacks attempted both by terrorists already present in Europe and teams of operatives deployed to the continent by one of the two quasi-state entities based on Turkey's borders. Both of these organisations threaten the West and have a track record of establishing and deploying attack cells for spectacular terrorist activities in Europe, most recently in Paris and Brussels. The two organisations are also directly responsible or jointly responsible for instigating or influencing the lion's share of the 134 successful and unsuccessful jihadi plots targeting Europe between 1990 and 2015, with ISIS overtaking Al-Qaeda in this role from 2012 onwards.

Between 2010 and 2014, ISIS, then called Islamic State of Iraq (ISI), transformed itself from a seemingly defeated Iraqi terrorist organisation into an international militant movement that combined features of a terrorist group, criminal syndicate, guerrilla army and a quasi-state. It branched out to other countries in the Middle East and North Africa and even in the Sahel and Libya, or incorporated existing jihadi organisations, such as Boko Haram in Nigeria and Ansar Bait al-Maqdis in Egypt, into its fold. Its success and territorial growth allowed for the development of a more globally oriented strategy that includes terrorist attacks in Europe. The territorial control ISIS now enjoys over parts of Syria and Iraq as well as in Libya enables it to prepare and direct attack cells to Europe. Such capabilities were beyond the organisation's reach before 2013/2014,

when it began a series of conquests in Iraq and Syria that led to the declaration of the "caliphate." The threat has been increasing since then and it is questionable whether the international anti-ISIS coalition will be able to reduce it because of the accumulated pool of trained fighters who have already returned to their home states or who are about to come back.

The international terrorist threat to Europe should not only be associated with entities and quasi-state actors beyond the continent's borders that have established terrorist networks on the continent and direct them but also with jihadists and jihadi sympathisers with no direct connections to these entities and living within European states. The external and internal character of the threat becomes clear when one assesses the makeup of ISIS attack cells. These consist of both local ISIS "wannabes" and returning veterans from the Syrian conflict, sometimes disguised as migrants or refugees. Such cells are capable of staging often spectacular but relatively rare terrorist attacks, after which they rapidly disintegrate because of personnel losses. At the same time, ISIS sympathisers in Europe who are not connected to the main body of the organisation attempt to stage individual terrorist attacks. Some of them are unsuccessful but they are usually less spectacular than the activities of the cells directed and led by the ISIS returnees.

Despite relatively optimistic predictions about the end of ISIS, the terrorist threat to Europe could actually increase. If the "caliphate" continues to shrink territorially in Syria and Iraq, it may no longer be a place ISIS sympathisers based in Europe would want to go. However, not joining the fight in Syria should not be automatically associated with an abandonment of plans to commit violent acts because these prospective jihadists could instead focus on attempting a terrorist attack in Europe. In the meantime, foreign fighters returning from Syria could also involve themselves in terrorist activities once back on their home continent. Terrorist attacks waged by these types may not be as sophisticated as an ISIS organised and directed plot, such as those in 2015 and 2016, but they could be more numerous and sometimes no less deadly. The threat against Europe from radical Islamist terrorism will not cease for years to come.

In relation to the terrorist threat, a novel phenomenon is the role played by the internet and social networks in radicalisation, a process by which future activists and fighters are being radicalised to embrace the terrorist ideology and follow it. Although the information sphere is full of disruptive ideologies, it seems that Islamist organisations have been relatively the most effective in using cyberspace-based tools to mobilise their supporters to not only finance terrorist activities and further spread the ideology but also to travel to join them, such as ISIS or Al-Qaeda (the so-called "foreign fighter" phenomenon). In extreme cases, such radicalised individuals also begin preparations for terror attacks on their home countries. The potential of radicalisation through websites, discussion forums or other social networks has to be, of course, put into a larger context. There are other factors that contribute to the radicalisation of individuals, among them, their material status and exposure to propagators of radical ideologies. Yet, the fact that popular internet tools, used by people to communicate with each other, are vastly exploited to spread hatred and violent political and social concepts, cannot be underestimated.

No one is questioning the importance of cyberspace to the security of the modern state and the capacity of cyberattacks to try to affect a country's external and internal policies, economy and everyday routines. Yet, the most disturbing trends in cyberspace remain underestimated and poorly understood. While cybercrime has become a notorious threat and no individual, business or state agency can consider itself safe from the many methods and attempts at fraud and data theft, it goes largely unnoticed that states have resolved to deploy hacking techniques in pursuit of their vital political and economic interests.

Until recently, the threats in cyberspace have been seen as mostly falling into one of the following categories: cybercrime (understood as attacks motivated by the desire to make money from illegal activity, mostly fraud), hacktivism (a manifestation of a public protest such as those demonstrated by the loosely connected hacker group Anonymous), cyberwarfare (a new domain

of military conflict), cyberterrorism (the use of electronic networks to perform terrorist attacks), and cyberespionage (a new way of spying). This compartmentation has, however, outlived its usefulness as states have re-sculpted the landscape of the threats in cyberspace.

As of 2016, what can be considered the most pressing threat from within this domain is "cybersabotage," which involves attacks on critical infrastructure (CI). For a long time, the security of Supervisory Control and Data Acquisition systems (SCADA), such as those managing processes in industrial plants, water and sewage networks, gas and oil pipelines, electric grids, railways or other highly-automatised transportation systems, have been seen as under threat mostly from individual hackers, motivated by psychological dysfunction, or terrorists. Despite the immense destructive potential of such attacks, which could easily lead to large material losses and casualties, there have been only individual cases of small-scale CI attacks perpetrated by either former or current employees of companies. What is more, the widely known campaign of cyberattacks against Estonia in 2007 showed that the cyberspace threat was more about denial of access to internet-based services and economic/political losses than physical damage. Large, damaging attacks against SCADA systems remained a near possibility, but not yet a reality.

The change came in 2010 with the Stuxnet worm, later described as the world's first "cyberweapon." Owing to the smart code that made it potentially lethal, it built upon a number of known vulnerabilities (security gaps in commercial software) and required significant manpower and time to be written. Stuxnet remained undetected for a long time, eventually making its way to its predefined target, in this case, Iran's Nantaz enrichment centre and its centrifuges, thousands of which were eventually broken by the malicious code, seriously impeding the country's uranium enrichment programme. There are strong signals, that Stuxnet was only the tip of the iceberg and that a number of states have similar cyberweapons at their disposal. This assumption was confirmed by the December 2015 paralysis of power grids in western Ukraine as a result of a targeted cyberattack. The consequence of the attacks were blackouts that directly affected more than 225,000 people and lasted several days in some areas. A link to foreign groups was indicated by Ukrainian authorities, yet, as is the case with all sophisticated cyberattacks, not proven by hard evidence. More importantly, though, even if there were no direct casualties because of those attacks, the potential for such manipulation is clearly alarming.

Both of these cases show that with SCADA systems now effectively being targeted, cybersabotage looms as a new primary threat in cyberspace. The ability of states to hide behind the ambiguity of global computer networks may tempt governments, particularly those in conflict with the international order, to reach for these types of instruments in search of political gain. It cannot be excluded that cybersabotage will accompany a political conflict and not necessarily be followed by the use of open military force. This possibility draws out questions about the possible reaction of the target, which may not have the capacity for a reciprocal response, i.e., one limited to cyberspace. It also indicates that despite a vast amount of theoretical work, the boundary between such an attack and overt aggression is blurred and is subject to political choice and consensus, rather than an objective evaluation. Cybersabotage also fits perfectly into the hybrid warfare concept, in which irregular, typically terrorist or criminal operations can be augmented with selective "strikes" on chosen CI elements. This is how cyberwarfare can be fought, and actually in some cases already is, even without open hostilities or political declarations. From the perspective of the Alliance, this raises an additional dimension, which is, in a hypothetical conflict, whether an effective attack on CI preceding a military escalation can be used as a tool to break the political will and the public's willingness to intervene. In other words, in looking at the threat from Russia, NATO has to take into account that hybrid warfare will include a strong cyberspace component that may directly result in the threat of material losses and casualties far from the contested area.

Meanwhile, in the popular discussion, the threat to Europe is more and more associated with the mass migration of people who are trying to seek safety and economic security in the wealthiest EU Member States. The failure to reach consensus within the EU on how to manage this unprecedented flow of refugees and other migrants, combined with the revealed shortcomings of European migration policy and border protection systems, has undermined European solidarity in a moment in which it is crucial to address the entire spectrum of threats in a more consensual manner. Further, the focus on the migration crisis as the key challenge for Europe misses the point about the nature of the threat looming in the backdrop. It is not only the breakdown of statehood and the economy in the Middle East and North Africa, exemplified by the collapse of two strategically important states—Syria and Libya—and subsequent destabilisation of a number of other states around the region, that causes mass migration but also long-term demographic and climate changes, which in Africa will inevitably lead to greater numbers of migrants seeking to go to Europe in the future. The current European stalemate on migration issue testifies as much to the inability of the EU to find a way for its members to agree to adjust its internal policies, as to the failure of its broader policy towards the Middle East and Africa.

If the mass-migration crisis is to be considered a threat to EU migration policies and possibly a further blow to the entire European integration project, its sources pose even a bigger danger. Mass migration is to a significant extent managed by international, organised criminal groups, which at the same time are likely to attempt trafficking drugs or weapons, including chemical and biological agents, which may be used as components of weapons of mass destruction, or trading illegally acquired raw materials, such as oil in Libya and Syria/Iraq. But more importantly, in the countries of origin, due to the outflow of people of productive age who are often also relatively well-educated, migration sets the stage for further destabilisation. For instance, this outflow led to the rise of Islamist militias in Libya and may lead to turning entire countries, such as the Central African Republic, into another Somalia. In other words, migration—now considered by mass media as a core security challenge of Europe—is only a symptom of a collapsing European neighbourhood, threatening it with a security vacuum, which in the longer run, if not addressed properly, is bound to generate far more threats than just thousands of migrants on Europe's borders.

III. Enhancing Deterrence and Defence on NATO's Eastern Flank

The upcoming NATO summit in Warsaw will conclude the initial phase of the Alliance's adaptation to the increasingly hostile European security environment. The process launched at the previous summit in Wales in 2014 has to a great extent constituted a response to Russian political-military posturing against NATO, with further steps expected to be adopted in Warsaw. These measures are undoubtedly considered the most politically divisive, just as they were proven to be two years ago.

Yet, since 2014, implementation of the Readiness Action Plan (RAP) allowed the Alliance to partially bolster NATO's collective defence capabilities. RAP did not, however, close NATO's vulnerabilities to Russian military superiority on the Alliance's Eastern Flank because it is built almost exclusively on the principle of reinforcement with a very limited, non-combat forward presence. The regional conventional imbalance, combined with Russian nuclear and hybrid capabilities, imperils not only the security of the easternmost NATO members but also the credibility of the Alliance and stability in Europe. Further, it demands that NATO develop proper military tools and concepts for the Eastern Flank in order to close the Alliance's vulnerability gaps in the region.

The Warsaw summit should see the launch of more comprehensive, longer-term political, military and institutional adaptation. NATO needs to establish a credible deterrence posture comprised of a multinational forward presence of combat forces, enhanced reinforcement capabilities, a nuclear deterrent adapted to Russia's nuclear re-emphasis, and an improved ability to counter hybrid threats. Robust deterrence also would be complementary and supportive, rather than contradictory, to a possible dialogue with Russia and would create more room for political manoeuvring during a potential crisis.

In RAP, the Alliance has been focused to date on the enhancement of its ability to reinforce the Allies during a crisis or a potential conflict. Within the NATO Response Force (NRF), the Alliance has set up a Very High Readiness Joint Task Force (VJTF), a 5,000-personnel-strong unit, deployable within 2–7 days' notice. Additionally, two other land brigades could be deployed within 30 and 45 days, respectively. Altogether, the recently enlarged NRF consists of 40,000 troops, including air, maritime, and special operations forces components.

In order to improve its command-and-control abilities in the region, NATO has been raising the readiness level of the headquarters of the Multinational Corps Northeast (MNC NE) in Szczecin, Poland, and established the headquarters of Multinational Division Southeast (MND SE) in Bucharest, Romania. A total of six NATO Force Integration Units (NFIUs), each with 20 staff from host nation and 20 from other NATO Allies, have been activated in Bulgaria, Estonia, Latvia, Lithuania, Poland and Romania, with two more to be set up in Slovakia and Hungary. These coordination cells are tasked with facilitating exercises and potential operational deployment of Allied forces.

In addition to these efforts, NATO has taken several reassurance measures in the region. The number of fighters participating in the Baltic Air Policing mission has increased from four to eight. The continuous presence of land, maritime and air forces has been established through joint exercises and bilateral rotational deployments of national units that train with local forces. The biggest contribution to this point has been provided by the U.S., which launched the European Reassurance Initiative (ERI) to fund its increased presence. The country has been, among other measures, constantly deploying company-sized units (150–200 troops) to Poland and each of the Baltic States. In 2015, the U.S. announced it would preposition a brigade-sized set of heavy equipment (250 tanks, infantry fighting vehicles and howitzers) in Central and Eastern Europe to facilitate training activities. In 2017, ERI's funding is planned to be quadrupled to $3.4 billion. It

would cover the cost of prepositioning combat equipment for an armoured brigade in Western Europe, along with division-level command and support, and a continuous rotational presence of a manned armoured brigade in Europe.

RAP has contributed to the level of reassurance of Alliance members and an improvement in rapid response capabilities, but NATO's basic military vulnerabilities vis-à-vis Russia are still unaddressed. The Russian forces decisively surpass those of the Alliance's easternmost members, both in terms of the number of troops and in many categories of equipment, such as heavy armour, aircraft and artillery. Despite its financial woes, Russia has been beefing up its forces even further and plans to create two armoured divisions in the Western Military District. In a potential crisis, Russia would also enjoy the advantage of numbers, strategic depth and time over NATO reinforcements. It would take two days to deploy the first elements of a brigade-sized VJTF once the 28 NATO members reach consensus on how to respond to the Russian actions. Meanwhile, through "snap" exercises, Russia has demonstrated its ability to surprise by rapidly mobilising and deploying thousands of troops within several hours. Additionally, Russian anti-access area denial (A2/AD) capabilities could impede the entry of NATO reinforcements to the region. Its A2/AD systems, such as long-range air defences, anti-ship missiles and land-attack cruise and ballistic missiles are deployed all along NATO's borders—in Kaliningrad Oblast, Crimea, the High North, and Eastern Mediterranean. A potential attack launched from Kaliningrad in the direction of Belarus could also quickly close the so-called "Suwałki Gap," the narrow stretch of the Polish-Lithuanian border constituting the only land connection between the Baltic States—the most exposed members of the Alliance—and the rest of NATO. Altogether, these capabilities could allow Russia to occupy Allied territory even before the arrival of NATO reinforcements and then to try to discourage the Alliance from launching a long and costly operation to retake lost areas.

The weaknesses and shortcomings in NATO's force posture on the Eastern Flank and its overall capacity to reinforce it are a factor widely considered to be inviting Russia to at least test the Alliance if not to try to undermine its credibility, solidarity and, at the end of the day, the U.S. ability to deliver on its alliance commitments. Currently, despite the reassurance measures and implementation of RAP, Russia may be lured by the prospect of achieving an inexpensive local victory in the Baltics, possibly without engaging in a direct conflict with the rest of the Allies, and—in the strategic sense—opening the door to a formal dismantling of the post-Cold War legal and political order in Europe. To counter this, NATO has to develop a credible deterrence and defence posture on the Eastern Flank and start to think about its *modus operandi* when it comes to effectively deterring Russia and, if needed, ensuring a successful defence against it.

The first steps towards building a credible defence and deterrence posture on the Eastern Flank can be taken at the Warsaw summit, following the preliminary decision of the Alliance on establishing an enhanced multinational rotational forward presence, taken in February 2016. If the new force, the modalities of which have not yet been set in detail, were to serve as an effective deterrent, it would require different organisation—and philosophy of action—than the forces currently present on the Eastern Flank, as they are focused on training and exercises and unprepared to take part in combat operations. To constitute a genuine deterrent, forward-deployed units must be fully equipped, supported by necessary enablers and logistics, and covered by the collective Allied planning and command chain. They also ought to be big enough to be able to cover areas threatened in the event of provocation. This presence of combat units would ensure that an attack against the easternmost Allies would be tantamount to an attack on the forces of the other NATO members. It would, therefore, significantly diminish the aggressor's possible prospect of achieving a swift victory while avoiding a conflict with the rest of NATO. Second, such units ideally should be large enough to be able to, together with local forces, at least delay the initial phase of an attack to provide time for reinforcements to arrive. Thus, company-sized deployments

in Poland and the Baltic States should be increased to at least the battalion level or, optimally and in a later stage, to a brigade level in each of those countries.

The credibility of the deterrence and defence posture of NATO on its Eastern Flank would also be improved by further upgrades of regional reception infrastructure, prepositioning combat-ready sets of equipment in forward areas, and enhancement of early warning and situational awareness abilities. The region needs a bigger focus from both joint and national intelligence, surveillance, and reconnaissance (ISR) assets, with the possible establishment of forward-operating bases for the NATO Airborne Warning and Control System (AWACS) and Alliance Ground Surveillance (AGS) aircraft. To protect arriving forces and those already in theatre from Russian A2/AD systems, NATO should develop a mix of offensive and defensive capabilities that would include especially stand-off weapons, submarines, cyber offensive measures, stealth aircraft, and air and missile defences. While the involvement of the most capable NATO members would be critical, nations in the region could also contribute to these efforts.

Finally, even with an enhanced forward presence on the Eastern Flank and the VJTF and NRF fully operational, what also might preclude the credibility of NATO's deterrence and defence posture is the overall Allied force structure. Due to the post-Cold War focus on out-of-area operations and deep cuts in European defence budgets, territorial defence capabilities among the NATO members have radically deteriorated, especially in the categories of heavy equipment. National forces are hampered by shortcomings in their readiness, deployability and sustainability. Until recently, there have been only a few large-scale live exercises. Consequently, the improvement of NATO's defence and deterrence force posture will depend greatly on an increase in defence expenditures in line with the Wales Investment Pledge of at least 2% of GDP. At the NATO Summit in Warsaw, the Wales pledge should be enhanced by an additional defence planning pledge that could help to properly address the existing shortfalls in high-end capabilities. An effective adaptation process also requires comprehensive and regularly updated planning and exercises involving complex Art. 5 scenarios. Finally, it is desirable to enhance interoperability, information-sharing and consultations with NATO partners in the region, namely Sweden and Finland. Due to these countries' geographic position, cooperation with them would be crucial for NATO in the event of a conflict in the Baltics.

Along with a strong conventional posture, NATO also must be able to deter threats from the higher and lower end of the threat spectrum. Over the past two years, Russia has intensified its nuclear signalling towards NATO. The Alliance has witnessed a disturbing rhetorical emphasis of nuclear capability by Russian politicians; provocative nuclear-capable heavy bomber patrols near the airspace of NATO allies and partners; and nuclear exercises, including surprise drills that show the close integration of Russia's nuclear and conventional forces. All of these activities were exceptional in number, frequency, scale, and complexity, and of a provocative nature in the post-Cold War period. In addition, Russia has continued to issue implicit and explicit nuclear threats as a response to the development of NATO's missile defences. At the Warsaw Summit, NATO should denounce Russia's irresponsible sabre-rattling and sharpen its own nuclear narrative by stating that the Alliance will not stand down in the face of nuclear threat and any use of such weapons will fundamentally change the nature of any conflict. In addition, the Alliance should ensure the effectiveness of NATO's nuclear deterrence in the changed security environment by taking into account the nuclear component of Russia's approach to conflict in Alliance planning and exercise routines; strengthening analytical and intelligence skills to read and react to Russia's nuclear messages; and, ensuring sufficient capabilities, operational proficiency, and the broadest possible participation of allies in the current nuclear arrangements.

As demonstrated during the conflict in Ukraine, Russia has developed a set of hybrid tactics that integrate conventional military actions and unconventional tools, such as covert special forces and intelligence operations, propaganda, cyberattacks, criminal and militant proxies, as well as

political and economic pressure. Its hybrid operations often rely on a denial of the aggressor's involvement, blur the lines between war, crisis, and peace, and may fall below the threshold of NATO's Art. 5 guarantees. As such, they might be used against NATO countries for the purpose of destabilisation and coercion, perhaps along with the exploitation of a supposed threat against Russian-speaking minorities in the Baltic States to justify an outright military intervention. Although the Alliance has a limited role in dealing with non-military challenges, which fall predominantly within the purview of national authorities, it should increase its support for its member states with expertise, special forces operations and sharing intelligence, surveillance data and other information. Allied decision-makers already have conducted exercises that include hybrid scenarios, but they need to take place regularly, at least once a year. NATO must also further enhance its strategic communications and cooperation with the EU, given the large degree of complementarity in the approaches of both organisations. NATO–EU collaboration should stress information-sharing, situational awareness, regular joint tabletop and live exercises, and the alignment of crisis-response procedures. Within this domain, addressing the cyberthreat properly is of utmost importance. To say the least, the Alliance has long lagged behind with regards to the acknowledgement of the importance of cybersecurity. Although cyberdefence received significant political attention from NATO at the 2002 summit in Prague, the Alliance adopted its first Cyber Defence Policy only in 2008, after a wave of cyberattacks paralysed government and private networks in Estonia. The policy was revised in 2011, and the current Enhanced Cyber Defence Policy was endorsed at the 2014 Wales Summit with an aim to provide an updated approach to a threat that increasingly moves towards an element of state-waged warfare.

Still, NATO's main task within the realm of cyberspace is the protection of its own networks, which link headquarters, agencies, other bodies and missions. Responsibility for protection of national networks rests upon the member states themselves. True, NATO has been enhancing its support for building up national cyberdefences and improving cooperation among the Allies through training, education, regular exercises, expertise, and facilitating the sharing of information and best practices. It also has set minimum security requirements for national networks critical for NATO tasks, established capability-development goals within the NATO Defence Planning Process (NDPP) and included cyber-related projects in its Smart Defence agenda. The Alliance also incorporates cyberdefence issues into operational planning and related exercises and strengthens its relations with partners, including from the private sector, which operates the majority of the world's information systems and critical infrastructure.

Nevertheless, in the now increasingly likely event of a significant cyberattack against an Ally, NATO can provide only limited assistance. Currently, it has just two six-person Rapid Reaction Teams (RRTs), deployable on the North Atlantic Council's (NAC) consent, although they could be further supported by national experts. In a move to close the gap of NATO's limited ability to actually reinforce an Ally that has become a victim of a cyberattack, the Alliance declared at the Wales summit that a cyberattack could lead to a collective defence response under Art. 5. The policy has, however, not defined the form of the response and the threshold that would trigger a collective reaction. While this ambiguity might enhance deterrence, especially against the most harmful cyberattacks, there is much more to be done to improve NATO's profile with regard to cybersecurity. Strengthening it would require the willingness of the Allies to invest in their cyberdefence capabilities and—first and foremost—cooperate closer with each other. The will to become serious about the matter could take the form of a "cyberdefence pledge," that is, a commitment to spend a specific part of member states' budgets on improving such capabilities. Another option is to shorten the planning cycles in the NDPP to better take into the account the dynamic evolution of technologies. NATO could declare cyberspace an operational domain and begin consultations and planning on the use of national cyber offensive measures for deterrence and warfighting purposes. There are, however, no quick fixes for building trust among the Allies, even if sharing information about their national capabilities and detected threats is necessary for

comprehensive planning, exercises and crisis response. The Alliance needs to address this hurdle if it is meant to stay relevant as regards genuine cyberdefence.

Facing Russia's openly revisionist policy aimed at dismantling the post-Cold War legal and political order in Europe through all means, including military tools, NATO has no other choice then to go for a robust deterrence and defence force posture. But it would be wrong to think that deterrence precludes dialogue and contributes to the escalation of tensions. Maintaining a persistent presence of rotating multinational forces on the Eastern Flank, supported by effectively implemented VJTF/NRF and augmented by a tested system of reinforcement build upon the reformed overall force posture of the Alliance, would allow more room for political manoeuvres in a time of a crisis. If deterrence can save the peace it does so precisely through military and political signalling, which, to be credible, requires proper tools. For instance, by beefing up already deployed forces, their movements, exercises or additional deployments of special assets, ready to be received thanks to developed host nation infrastructure, NATO could prevent a potential political crisis from spilling over to the military domain. Deprived of assets that could be effectively used as tools of political-strategic signalling, NATO could be forced in a time of crisis to take a binary choice—remain at the political level or directly go to Art. 5. In this sense, a robust deterrence and defence posture actually makes it less probable that Russia and NATO move to a military standoff.

Nevertheless, NATO should also keep political and military channels of communication open for possible contact that would de-escalate tensions or allow the avoidance of military incidents. Even if this dialogue has not proved of much value yet—Russia seems disinterested in greater military transparency, as the lack thereof makes it easier for it to reinforce its political signalling through snap exercises and to cloud its force movements—it has to be kept as an open option as Russian interest in such arrangements might grow along with the enhancement of the Allied military posture. This does not mean that a credible NATO defence and deterrence posture will guarantee a successful dialogue, but dialogue with Russia is unlikely to be successful if not backed by a robust military posture.

IV. Reinforced Partnerships and Specialisation: How to Tackle Asymmetric and Non-Military Threats

Although the optimal way forward for NATO in countering the Russian threat to the Eastern Flank is well defined and the main limitation for implementing it is of a political nature, the asymmetric and non-military nature of the threats coming from the broader neighbourhood of the transatlantic area requires further conceptual work. The Alliance needs to re-examine its philosophy of how to approach these threats because presently it has neither the optimal toolbox nor rich experiences to draw on. The principle behind this reflection should be to remain selective and to look for partnerships with individual countries, organisations—principally, the European Union—and other coalitions better equipped than NATO to solve compound crises in which security is only part of a larger problem.

Still, NATO has the capacity to be of primary importance in addressing some of the asymmetric threats. One such case regards high-intensity crisis-management operations. NATO might or might not be involved in such actions in the future, depending on actual contingencies and the collective will of the Allies. Nonetheless, NATO should maintain, and in some areas improve, related capabilities, in order to provide adequate military options if needed. It is possible that due to their political and operational flexibility, "coalitions of the willing" will be seen as preferable to acting within the framework of NATO, but the Alliance also has its own advantages in terms of command-and-control structures, fit for the coordination of larger operations, or joint capabilities that could be utilised also by NATO as part of a broader coalition.

Second, NATO has a key role to play in the field of missile defence. The ongoing proliferation of ballistic missiles poses a significant risk to NATO nations, and potential threats might arise from both state and non-state actors. One of the main concerns relates to Iran, which continues to improve its ballistic missile arsenal and has recently stepped up test launches of such systems, some of which are already capable of reaching the southern members of NATO. While the conclusion of a nuclear deal in 2015 has been a promising step, the future of its implementation is not certain. Moreover, the agreement does not prohibit the development of ballistic missiles armed with conventional warheads, and the possibility of Iran's actual or future possession of chemical and biological payloads cannot be excluded. Hence, the Alliance should proceed with the establishment of its Ballistic Missile Defence Capability, including the activation of the U.S. Aegis Ashore site in Poland in 2018, which would extend the system's coverage to all of Europe.

Of the Alliance's many partnerships, its strategic relations with the EU are of utmost importance. Both organisations are founded on the same Western values, share 22 members and security environment, and together possess a wide spectrum of different policy tools. While NATO has been discussing next steps in its adaptation, with eventual decisions to be taken at the Warsaw summit in July, the EU has been working on its Global Strategy, which will be presented at the European Council meeting in June. This timing creates an excellent opportunity for NATO and the EU to bolster their strategic relationship and present a lasting common vision in tackling security challenges. One of the main tasks of this reinforced partnership should be to cope with the fall of state structures and economies in the MENA region, the core source of much of the recent migration to Europe, as well as with Islamist terrorism, which is thriving due to the rise of ISIS. Also, cyberthreats and, more broadly, hybrid warfare constitute promising areas for coordination and burden-sharing. Yet, NATO should stay focused on its core competence so that the broader toolbox of EU policies can be reinforced by NATO's unique set of assets and experience rather than substitute or duplicate efforts.

The task of stabilising Libya and Syria—two of the biggest sources of asymmetric and non-military threats to Europe—will require an effort greater than the EU's capabilities, particularly with regard to establishing future "national unity" governments. Also, the rebuilding of state structures and the economies of these countries that would follow any political deal will be a broad task and require more involvement than just the EU. What NATO could contribute, for instance, is the restoration of the security sector through military or police training, such as the barely remembered training mission to Iraq (NTM-I, active from 2004 to 2009). Further assistance would include enhancing situational awareness regarding sea or land borders using specialised Allied capabilities. Even if the first condition for such engagement, namely the political consent, is not yet met in either Syria or Iraq, NATO can already begin preparing assets for such activities, particularly since there may be other countries in the MENA region that might be interested in such cooperation with the Alliance.

Another possible tool that NATO should consider in this regard would be a new standing NATO training/operational force based on military police. Such a force would be cheaper to sustain than the highly specialised and high-intensity-operation-fit rapid-deployment troops that form the core of NRF/VJTF. It could be used more freely outside NATO territory for the advancement of defence capacity building initiatives (DCBI) and offered to partner countries in the MENA region. This could also allow somewhat greater flexibility in responding to asymmetric threats such as the advance of Islamist terrorist or militia groups in failed or weak states. Such forces could also effectively work alongside a potential EU civilian mission, for example, one focused on Security Sector Reform or building the capacity of the justice system. NATO and the EU share the common experience of simultaneous deployments in the same theatres (Kosovo, Afghanistan) and numerous lessons have been learned that should be implemented in the event of a similar "double deployment" in the future. This also means that any parallel missions could be better coordinated and mutually reinforcing, unlike when NATO and the EU were only learning how to work hand-in-hand on crisis management. What is enticing is that such coordination may also work if the political stalemate within the Alliance due to the Turkish-Cypriot cross-vetoes is not solved (although there are signs that the Cyprus conflict can be solved soon).

The same is true for counterterrorism policy, with a focus on foreign theatres and cybersecurity. The EU established a Counterterrorism Coordinator (CTC), which carved a niche for itself in the EU's outreach to its external, mostly southern, partners who suffer acute terrorism problems. NATO could develop a similar position and make its coordination partner the CTC while focusing, for example, on capacity-building for counterterrorism forces of MENA countries. The two could work well together, with the CTC responsible for civilian or non-military aspects of the EU's aid package to its partners and the NATO coordinator focused on military elements of the CT package offered to neighbours and allies.

With regard to cyberspace, the EU–NATO cooperation also needs to be further enhanced. The approaches of both organisations are largely complementary, with NATO focused on military aspects and the EU concentrated on non-military issues, particularly protection of critical infrastructure, countering cybercrime, and network and information security. There are also partial overlaps, especially given the EU's limited interest in cyberdefence. To strengthen prevention and response to attacks, NATO and the EU should enhance information-sharing, and conduct joint exercises. They also should avoid duplication of efforts and save resources through joint capability development and greater mutual use of existing assets in the areas of education and training.

What is perhaps most important, however, is that the partnership with the EU should focus on the use of hybrid warfare tactics on the modern battlefield. Even if there is no widespread agreement regarding the exact meaning of the term, there is an understanding that such methods involve a number of instruments related to the use of force. It seems that traditional military force remains a core element of hybrid warfare, but it is supported by a mix of other tools, all well-

known but combined in a novel way, including covert operations, acts of terrorism, criminal activity, disinformation campaigns and cyberattacks. Further, hybrid warfare means that wars also can be fought by proxies to a greater extent than was possible in the past and that these proxies can take a different form than has been recognised in military doctrines focused on counter-insurgency operations. This implies the limited applicability of classical military force in countering them. If a hybrid conflict starts with, for instance, staged popular unrest and a mass disinformation campaign, and then is supported by cyberattacks, the role of the military can be limited to deterring the orchestrating actor in such a crisis from further escalation.

This is precisely how NATO is—gradually—channelling its thinking about the potential of Russian hybrid-style provocations in the Baltic States. Crucial as it is to the potential for de-escalation, military force will be insufficient to actually solve the crisis and probably will not be of much use for detecting signs of a hybrid operation's preparations. Here, typically civilian capabilities come into play: intelligence-sharing, police cooperation, border reinforcements, cyberspace protection, etc. None of these can be effectively addressed by NATO alone, but the EU already has a rich record in this regard. Consequently, the EU and NATO should develop a common approach to hybrid warfare, with predefined areas of responsibility and—perhaps most importantly—robust channels and procedures of coordination of their actions. It is more than likely that almost all future conflicts will have a hybrid character, and therefore the EU–NATO strategic partnership in this domain may provide the impetus for a larger process of re-crafting the mechanisms and philosophy of both organisations to simultaneously tackle an unfolding crisis.

There also other partners, apart from the EU, that could offer clear added value and strategic opportunity for the Alliance. Among them are individual states, both those that share a membership perspective and those that have chosen to partner with the Alliance because of close strategic interests or guiding political values. If NATO is to assume a tailored approach, it also has to make such partnerships deliver in key areas that contribute to the strengthening of cooperative security as guided by the Alliance.

As regards enlargement of the Alliance, the doors must be kept open for all potential members, but at the same time, NATO should engage them now in even closer military cooperation to address the imminent security threats to Europe. To improve the security of the Eastern Flank, close collaboration with Finland and Sweden is instrumental for all the reasons described above, including Russian regional military superiority. When it comes to a broader policy of deterring Russia, increasing the stability of Ukraine and Georgia, both through a genuine membership perspective and the use of specially designed military programmes involving more training and exercises, is, again, a crucial task. Broader NATO partnerships under the Mediterranean Dialogue, Istanbul Cooperation Initiative or global partnership formula, should be further explored to allow NATO to have an enabling role in building a stable neighbourhood around Europe.

PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

The Polish Institute of International Affairs (PISM) is one of the most influential government-affiliated research institutes worldwide. It promotes the flow of ideas that inform and enhance the foreign policy of Poland. PISM provides independent analysis and advice to all branches of government, contributes to wider debates on international relations and houses one of the best specialist libraries in Central Europe.

ISBN 978-83-64895-79-1 (pb)
ISBN 978-83-64895-80-7 (pdf)