NATO Countering the Hybrid Threat

BY MICHAEL AARONSON, SVERRE DIESSEN, YVES DE KERMABON, MARY BETH LONG, AND MICHAEL MIKLAUCIC

The North Atlantic Treaty Organization (NATO) was the most successful collective security arrangement among states in the 20th century. Having deterred and outlasted its primary adversary, the Soviet Union, NATO now faces the challenge of redefining its roles and purposes in the 21st century. Like all pluralist organizations, the Alliance must reflect the common interests of its 28 members, and defining common interests that motivate all members to sacrifice for the good of the whole has been difficult. In the absence of a direct common military threat, disparate interests, commitments, and visions of the transatlantic future have fragmented Alliance coherence.

The Strategic Concept adopted by heads of state and government in Lisbon in November 2010 reconfirms the NATO commitment to "deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole."[1] It offers itself as the strategic map for NATO in the 21st century and touches on extremism, terrorism, and such transnational illegal activities as trafficking in arms, narcotics, and people, as well as cyber attacks and other technological and environmental threats. The Strategic Concept, however, does not refer to hybrid threats or provide insight into the magnitude, likelihood, nature, or nuances of the "emerging security challenges." Moreover, it does not address the possibility of having to face some or many of these challenges simultaneously, or the threat posed by the convergence of these many separate elements, which when braided together constitute a threat of a different nature.

The new threat confronting the diverse nations of the Alliance is insidious and not easily defined or identified. It flourishes in the seams *between* states, and in the soft areas of bad or weak governance. The new threat consists of distinct but tangled elements—hence the rubric *hybrid*

Michael Aaronson is a former United Kingdom Ambassador. Sverre Diessen is a Major General in the Norwegian Armed Forces. Yves de Kermabon is a Lieutenant General in the French Armed Forces. Mary Beth Long is a former U.S. Assistant Secretary of Defense. Michael Miklaucic is Director of Research in the Center for Complex Operations.

threat. Hybrid threats are much more than the amalgamation of existing security challenges. This is due in part to the interrelatedness of their constituent elements, the complicated and interdependent nature of the activities required to counter them, the multiplicity of key stakeholders with vested interests, and the dynamic international security environment in which traditional military solutions may not be best (or even a key component) but may nevertheless be necessary. As NATO Secretary General Anders Fogh Rasmussen has recently stated, "The paradox . . . is that the global order enjoys more stakeholders than ever before, and yet it has very few guarantors."[2]

The task of articulating, elaborating, and developing these concepts has been assigned to NATO Allied Command Transformation (ACT). In the words of one NATO/ACT official, the task is to "paint the face on the faceless enemy"[3] and to develop the hybrid threat concept, as well as examine viable and effective strategies to meet hybrid threats. A recent experiment raised important issues concerning how NATO does business. One of the issues raised was how NATO reaches out to important civilian players who it may have to rely on or even support in its current and future endeavors. Another topic was how the Alliance engages with industry, particularly with the cyber and energy sectors as two key areas identified in the Strategic Concept. Yet another issue is how NATO deals with nonmilitary threats that are nevertheless security dangers to the Alliance but do not lend themselves easily to the traditional Article 5 analysis. Lastly, the experiment asked whether NATO bureaucracy and its processes have kept pace with a rapidly changing world; or whether the Alliance is positioned to respond effectively to the frightening pace of emerging security threats.

the new threat confronting the Alliance flourishes in the seams *between* states, and in the soft areas of bad or weak governance

NATO in the 21st Century

As NATO positions itself to meet the diverse and complex security challenges of the 21st century, it must carefully take stock of the needs of all its members. In examining emerging threats, the following points are salient:

- We need to be as secure against emerging threats as we were against the conventional threats of the past.
- NATO was appropriate for security against past (that is, conventional) threats.
- Its effectiveness against emerging threats should not be taken for granted and must be demonstrated.
- We must understand the nature of the new threats.
- We must discover how these threats can be effectively countered.
- We must determine what role, if any, NATO can play in countering these threats.

NATO operates by consensus; it has only been the presence of an existential clearly identifiable threat (the Soviet Union) that allowed the Alliance to operate effectively over the years. Because hybrid threats are not clearly identifiable and their existential nature is not the subject of consensus, there is never an

imperative to address the challenge they pose. One way of framing the issue, therefore, is to say that we must demonstrate the existential nature of the current threat or threats to provoke a discussion and decision about how NATO wishes to respond. Without this, the discussion will continue to fall prey to conflicting visions for NATO within the Alliance.

NATO nations are all members of the United Nations (UN), and most belong to the European Union (EU). So for any NATO member, the starting point in the discussion will not necessarily be who NATO needs to work with to counter emerging or hybrid threats, but rather to what extent states want to work through NATO as opposed to individually, or through the UN, the EU, or other alliances. NATO action is complicated by the blurred distinction between legality and legitimacy in an Alliance intervention where there is no clear and unambiguous Article 5 justification.

The 1999 Kosovo intervention, for example, was widely perceived as morally justified and therefore legitimate when compared to nonintervention. Legality, on the other hand, will by definition depend on a Security Council resolution sanctioning military intervention by the international community. Despite the possibility of the Security Council acting in what may be the political interest of its member nations without being strictly moral by universal standards, it is generally accepted that Security Council–sanctioned action is legitimate by definition. In other words, all legal actions are legitimate, whereas the opposite is not necessarily true. Or, to put it another way, legality is a subset of legitimacy, and legitimacy is not for NATO alone to determine. Allied leadership acknowledges this: "The UN Security Council must remain the overall source of legitimacy for international peace and stability."[4]

Since it is widely held that UN sanction is a prerequisite for any kind of legitimate civil-military intervention, NATO's level of ambition will be effectively limited by what the least willing member country can agree to. This, in turn, is decided by the degree of necessity from the point of view of the country least threatened, or by the member for whom intervention policies are most difficult for domestic political reasons. This dynamic has been clearly brought out by the current NATO intervention in the Libyan conflict. This may raise doubt about the ability of NATO to deal with hybrid threats, other than as a forum for the creation of coalitions of the (most) willing—provided there is also the necessary legitimacy.

since UN sanction is a prerequisite for legitimate civil-military intervention, NATO's level of ambition will be effectively limited by what the least willing member can agree to

This leads inevitably to NATO's role, if any, in non–Article 5 situations in which the Alliance or a member is threatened in nontraditional ways. Emerging threats in the technology or cyber realm offer interesting examples. At what point does a cyber attack become a threat to the Alliance or its members? Certain scenarios are relatively straightforward. For example, if NATO or one of its facilities was assaulted by cyber attackers, the Alliance could not only defend itself, but also engage in offensive-defense actions to identify, mitigate, contain, and retaliate against such an attack. Similarly, if a member state were under cyber attack and requested Alliance assistance, this would be an appropriate use of its power and resources.

Former Defense Secretary Robert Gates and international leaders attend NATO and non-NATO ISAF contributing nations meeting in Brussels

DOD (Cherie Cullen)

Other plausible scenarios are less clear, however. What if a member nation's cyber security posture was so poor that it represented a threat to the Alliance due to its interconnectivity with vital Alliance facilities or activities? Who would be responsible for improving that state's capacity, deterring attack, responding to an attack, or repairing the damage done by an attack? How might a member under internal attack invoke NATO action in the case of a cyber or other technology-driven assault, particularly one deemed to fall short of Article 5 parameters? Who would be responsible for identifying the attacker? Does it matter that a hybrid threat might originate either in capabilities only residing in nation-states, or would NATO also pursue private citizens, cyber hackers, or criminal enterprises that threatened Alliance or member cyber security? Does the Alliance have the tools, expertise, and mandate to do so? Do changes need to be made to the Alliance's core processes and procedures to respond to emerging and fast-paced threats? Is there a need to identify possible instances when the "consensus" model should give way, allowing a more flexible "coalition of the willing" response to security needs?

The Hybrid Threat

Threats are the combination of our weakness and the enemy's intent and strength. It is important that we keep the language right. The last thing we want is a "War on Hybrid Threats." There is an urgent need to carefully analyze the range of threats confronting our world to better prepare our defenses. What is the difference between a real threat and mere fear or concern? This is the first question NATO must examine. Is there such a thing as a hybrid threat, or is this merely a new

way of looking at threats that have existed for a long time? While many of these threats are not new, they have now become more frequent and are manifested in novel ways. Does their combination, simultaneity, or perpetration by a single adversary or group of adversaries constitute a new and present danger? One must then determine when these threats become seriously dangerous and when they might require a reaction from the international community. What actions should trigger a concrete reaction?

Admittedly, *hybrid threat* is an umbrella term encompassing a wide variety of existing adverse circumstances and actions, such as terrorism, migration, piracy, corruption, ethnic conflict, and so forth. What is new, however, is the possibility of NATO facing *the adaptive and systematic use of such means singularly and in combination by adversaries in pursuit of long-term political objectives*, as opposed to their more random occurrence, driven by coincidental factors. It is this possibility that merits a fresh and more conceptual approach from NATO's side as to how they can be countered. It is particularly important to note that hybrid threats are not exclusively a tool of asymmetric or nonstate actors, but can be applied by state and nonstate actors alike. The principal attraction of hybrid threats from the point of view of a state actor is that they can be largely nonattributable, and therefore applied in situations where more overt action is ruled out for any number of reasons.

According to the most recent iteration of the NATO Capstone Concept, "Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[5] By not specifying state adversaries, this definition acknowledges both the ambiguity of the enemy and the simultaneous and combined conventional and unconventional nature of the threat itself. Clearly, the traditional boundaries defining the conflicts that served as the basis for the Alliance's historic shared interests do not apply today. It is no longer true that only the most powerful states have the means and intention of posing a dire security threat to the Alliance or its members. The means of destruction have proliferated from the few to the many, with the barriers to entry for some technologies and methods capable of wrecking havoc relatively low or nearly nonexistent. As noted, adversaries capable of threatening NATO and its members need not be government actors; nonstate and anonymous actors can and do pose a substantial threat. Security threats are no longer bound by geography and can have impact on a substate or worldwide basis. They are not even bound by terrestrial limits and may manifest themselves in space or cyberspace against Alliance interests or against NATO itself. Deadly and devastating attacks against Alliance members can be perpetrated and initiated in an instant from remote locations, leaving no trail to determine their origin.

NATO/ACT is far from alone in trying to identify and articulate this new generation of threat and to develop effective strategies to mitigate hybrid threats. Significantly, NATO efforts track U.S. attempts to paint a face on the faceless enemy, develop conceptual clarity on the nature of the threat, and develop capabilities to counter the threat. The 2008 U.S. Department of Defense Directive 3000.07, "Irregular Warfare," defines its subject as a "violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. . . . It may employ the full range of military and other capacities in order to erode an adversary's power."[6] The *National Strategy*

to Combat Transnational Organized Crime, subtitled *Addressing Converging Threats to National Security*, states that its subject, transnational organized crime:

> *threatens U.S. interests by taking advantage of failed states or contested spaces; forging alliances with corrupt foreign government officials and some foreign intelligence services; destabilizing political, financial, and security institutions in fragile states; undermining competition in world strategic markets; using cyber technologies and other methods to perpetrate sophisticated frauds; creating the potential for the transfer of weapons of mass destruction (WMD) to terrorists; and expanding narco-trafficking and human and weapons smuggling networks. Terrorists and insurgents increasingly are turning to criminal networks to generate funding and acquire logistical support. Transnational organized crime also threatens the interconnected trading, transportation, and transactional systems that move people and commerce throughout the global economy and across our borders.*
>
> *While the crime-terror nexus is still mostly opportunistic, this nexus is critical nonetheless, especially if it were to involve the successful criminal transfer of WMD material to terrorists or their penetration of human smuggling networks as a means for terrorists to enter the United States.*[7]

it would be detrimental to NATO long-term interests to fall too far behind its dominant member in understanding the nature of hybrid threats

These U.S. efforts reflect a growing awareness of the wide range of threat elements that over the past two decades have begun to converge and expand via globalization and new technologies in information access, communication, and transportation. The organizations, both state and nonstate, that operate in the nether networks of illicit commerce, terrorism, and insurgency have proven adaptable, innovative, and entrepreneurial as they have apparently begun to blend and diversify. They are "highly adaptive and show a great ability to learn and adjust their behaviors based on lessons learned and changes in the operational environment."[8] For a range of reasons, it would be detrimental to NATO long-term interests to fall too far behind its dominant member in understanding the nature of hybrid threats, anticipating their emergence, and developing countering strategies.

The Comprehensive Approach

The organizations, individuals, and networks that animate the hybrid threat "employ a complex blend of means that includes the orchestration of diplomacy, political interaction, humanitarian aid, social pressures, economic development, savvy use of the media and military force."[9] In short, they avail themselves of a comprehensive range of methods and weapons to accomplish their objectives—a comprehensive approach to goal attainment.

What changes in structure, process, and procedure might NATO adopt to account for the recent evolution of the international security environment and enable the Alliance to respond effectively to the comprehensive range of methods and weapons employed by hybrid

threat adversaries? Put simply by a NATO/ACT officer, "There are areas where we are not joined up and this can be exploited by others with harmful intent."[10] NATO Assistant Secretary General Jamie Shea elaborated that threats develop in response to vulnerability; we therefore need to understand ourselves better as well as understanding our adversaries if we are to respond effectively. This dual focus—looking inward at ourselves as well as outward at potential enemies—is an essential part of countering hybrid threats.

Countering hybrid threats is about new understanding of such threats and the innovative use of existing capabilities to meet these new challenges, rather than about new hardware. Indeed, the relevant countermeasures are largely included in the existing Comprehensive Approach to strategy, a concept NATO has embraced. This may be seen to imply that NATO has developed the solution to the problem before having defined the problem. However, the current understanding of the Comprehensive Approach is heavily influenced by the conflict that brought it about, as is often the case with innovation in the field of strategy. NATO therefore needs a more generic and conceptual grip on the kind of hybrid threat/comprehensive response cycle of which Afghanistan is but one example.

The recently adopted Strategic Concept states that:

> *The lessons learned from NATO operations, in particular in Afghanistan and the Western Balkans, make it clear that a comprehensive political, civilian and military approach is necessary for effective crisis management. The Alliance will engage actively with other international actors before, during and after crises to encourage collaborative analysis, planning and conduct of activities on the ground, in order to maximise coherence and effectiveness of the overall international effort.*[11]

The Comprehensive Approach thus begins to address the challenge, but how should we define this concept? Which agent or combination of agents provides the best response depending on the timing, nature, and place of the threat? How should the actions of various players be coordinated?

it is currently impossible to identify an international institution capable of coordinating all the efforts required to meet hybrid threats

One thing is clear: the Alliance cannot provide a credible answer on its own and currently offers only part of the solution to the problem. As a military alliance, NATO recognizes that it cannot implement a comprehensive approach and is limited to a supporting role. But who or what will it be supporting? A recent study of member perspectives on the Comprehensive Approach concept found three consistent themes:

- coherent application of national instruments of power
- comprehensive interaction with other actors
- comprehensive action in all domains and elements of crises.[12]

While these consistent themes emerge, the concept remains relatively undeveloped. It is currently impossible to identify an international

ISAF

As part of Afghan-led 2-day course at Kabul Military Training Center, trainees take target practice with M–16 rifles

institution capable of coordinating all the efforts required to meet the challenges of a comprehensive approach to hybrid threats. Though this is a difficult and sensitive issue, it would nevertheless be useful to bring a variety of capabilities from different contributors to a single organization. But what would be its mandate and legal framework, and how would one ensure that it was recognized by all as the overall coordinator? It seems that much time and patience will be required (as they were for the creation of the United Nations) before a solution is identified. In the meantime, several intermediate solutions are possible, such as what we call coalitions of the willing.

Beyond such intermediate steps, it is equally unclear what entities are best positioned to undertake the next steps toward policy development and implementation of the soft power tools contemplated by NATO's new Strategic Concept under the rubric of the Comprehensive Approach. The tools for economic development, such as rule of law, governance- and institution-building, and other "comprehensive activities," traditionally reside in nonmilitary governmental agencies, intergovernmental agencies, nongovernmental organizations (NGOs), and the private sector. These capabilities are not found either in member nations' militaries or in the NATO bureaucracy itself. Moreover, the civilian organizations or actors best equipped to provide them are frequently wary of the military. Most are unaccustomed to working with the military, at best. At worst, there are hostile feelings.

To overcome many civilians' lack of familiarity with working with NATO, one of the lessons learned from Afghanistan and Kosovo is that where the military and civilian sectors must work together, the military must often take the initiative to establish trust and communication

with civilian counterparts. The two communities work best when they work collaboratively and cooperatively. Collaboration and cooperation should begin with a shared analysis. All participants in a comprehensive approach must understand the challenge not only from their own vantage points, but from those of the other major participants. Many perceived threats (terrorism, transnational crime, violent extremism) are symptoms or consequences of underlying root causes (poverty, ethnic strife) that are not within the technical competence of most military organizations.

Whereas treating the symptoms is about *preventing actions in the shorter term*, addressing the root causes of instability is about *changing conditions in the longer term*, which is the fundamental goal of development. Removing the root causes of conflict is always more difficult and time-consuming than dealing with the symptoms. Long-term solutions aimed at solving the fundamental problems are also harder in terms of achieving the necessary political consensus at the national as well as the international or coalition level. This is a challenge of political agreement and thus of diplomacy. This means that in the absence of a political agreement, NATO may have to accept that treating the symptoms, despite its limitations, is the best buy under the circumstances. Even in such cases, the participation of nonmilitary organizations will enrich the military's understanding of the challenges they face.

As for planning, while the military may be best equipped to plan and facilitate the cooperation through planning and outreach, the civilian sector should be included in the earliest aspects of the planning for best results. Outreach should be done early and often to permit the civilians the necessary time for budgetary and other preparation. It should not be left to commanders on the ground to begin the search and engagement for the nonmilitary capabilities and partners they may need.

Once initiated, an effective comprehensive approach requires unity of effort, which in its turn requires at least some unity of command. This raises the question of who owns the problem, or more specifically what or where the organization, body, or entity is that can coordinate all the necessary means of persuasion as well as coercion to achieve the strategic objectives of the international community. We believe that if we do not all own it, we are in trouble. However, this is not the same as saying we need unity of command. The challenge is *how* to achieve unity of effort in the *absence* of unity of command.

the absence of unity of command does not exclude any possibility of success, but it means that achieving it will require more time, treasure, and potentially lives

Is it possible on a case-by-case basis to create a "supreme commander" who, assisted by a "comprehensive headquarters," can develop and execute campaign plans that encompass all necessary lines of operation, military and civilian? This seems highly unlikely. Many NGOs reject any kind of inclusion in coordinated strategies, particularly when they involve the military since that violates their principle of strict neutrality in any conflict. Other factors are bureaucratic rivalry between the different governmental agencies and departments which must necessarily contribute to a comprehensive effort, lack of trust between public sector agencies and private sector participants, and national sensitivities at the coalition level. One

practical implication of this is a lack of willingness to share intelligence, which may impede a coordinated effort in a theater of operations.

The overall effect of the absence of unity of command is a considerable dissipation of energy and effect for a comprehensive approach strategy. This does not exclude any possibility of success, but it certainly means that achieving it will require more time, treasure, and potentially lives. However, it seems a firm conclusion that unity of command cannot be achieved, at least not unless and until the group of nations forming the coalition faces an immediate existential threat. A comprehensive approach to hybrid threats is, in other words, as much an institutional as a conceptual problem. There will never be a single overarching goal to which all actors can be expected to subscribe. It is better to acknowledge that different actors in the same situation have different perspectives and seek the common ground that can form a basis for collaboration.

NATO needs institutions capable of making precise appreciations of the nonmaterialistic dimension of the root causes of hybrid threats

There is much discussion of whether NATO needs new capabilities to counter terrorism, cyber attack, transnational organized crime, insurgency, and so forth. Countering hybrid threats is first of all about new understanding of such threats and the innovative use of existing capabilities to meet these new challenges, rather than about new hardware. New equipment and weapon systems are not in this case the key to success. The challenge is to get better collaboration around existing capabilities.

A relatively unexamined component of the Comprehensive Approach is the question of strategic communications—at least when we consider its huge importance for the success of any such campaign. The execution of a diversified hybrid threat by an adaptive and intelligent adversary is first of all an acknowledgment of NATO's conventional military supremacy. Reverting to a hybrid (or comprehensive) approach on the part of the aggressor thus has two essential purposes:

- blurring the strategic picture by replacing a clearly visible friend-foe, good-bad perspective with a hazy multitude of actors and causes, thereby clouding the perception of what is at stake and who is behind it
- avoiding a situation where the issue is decided quickly through decisive use of NATO's overwhelming military capability by changing it into a protracted test of patience and determination as the campaign drags on with a steady toll of treasure and human lives and apparently no end in sight.

Both purposes make strategic communication and information to the public a matter of the utmost importance, if a comprehensive approach is to succeed. Real situation awareness must be created by presenting a credible picture of who the adversary is and what his long-term objectives are in order to justify intervention. Furthermore, the public must be given a clear and unambiguous understanding of the time scale of any comprehensive campaign aimed at defeating the threat. As has been proved by the Afghanistan War, the prevailing perception within the general public about the duration of armed conflict is still shaped

by the conventional war experiences of the major conflicts of the 20th century. This means on average that after 4 to 5 years, the "bring the boys home" campaigns and the "negotiate now" advocates will gain support as frustration and impatience start spreading. However, stabilization or counterinsurgency campaigns may take two or three times what a conventional war might. The public must therefore never be left in doubt as to what it is in for. If political leaders allow themselves to create false hopes by underestimating either the duration or the cost, the effect will reinforce the downturn in public support.

What Role for the Private Sector?

Arguably the single most important factor in successful stabilization of failed or failing states is economic development. That, in turn, depends on financial incentives to investors, improvement of infrastructure (digital as well as physical), access to energy, and a skilled workforce. This makes institutions such as the International Monetary Fund and World Bank key players and potential partners with NATO. This assessment, however, requires some qualification. Although economic development is obviously of the utmost importance in many scenarios, we should bear in mind that the Western materialistic definition of development is not a universally accepted standard of welfare or happiness. Notably, religion and adherence to religious customs are on the rise as the most important metric of human progress, particularly in the Muslim world. In other words, not all root causes of hybrid threats can be eliminated simply by improving the material living standards of the people in question. The rage felt by many Muslims toward the West—irrational as it may or may not be and sustained as it is by conditions stemming from the incompetence and corruption of their own governments—is nevertheless real. NATO therefore needs to partner with, or else have in-house institutions capable of making precise appreciations of the nonmaterialistic dimension of the root causes of hybrid threats. It is also interesting that many people living in poverty and squalor around the world rank competent and honest government as more important in the short term than a larger income, presumably because they realize that good governance is a prerequisite for any degree of sustained economic growth.

The Afghanistan experience has brought out an interesting dilemma when it comes to how we should prioritize resources for the achievement of economic development. Should the resources required to stimulate economic growth be applied where security as well as other conditions favor it, or should they be used in the most marginal areas, where presumably the need is greater and even modest progress can help turn the population away from an insurgent or destabilizing influence? In other words, should we apply military logic and reinforce success or try to stem the tide of destabilization by aiding those who, because they are most in need, may also be those most ready to reject insurgent influence? There is no hard and fast answer, but again it is an important aspect of designing a comprehensive strategy to defeat a hybrid threat. With these caveats, there is little doubt that economic development and progress is a powerful weapon in the NATO inventory, particularly in addressing root causes.

NGOs and industry have been dealing with some of the issues and many of the geographies of interest to NATO for much longer than the Alliance. Indeed, the private sector's individual companies feel the harm done by hybrid threat elements most directly. Counterfeiting networks

steal the intellectual property and potential revenues from legitimate companies. Cyber attackers can disable information and communication companies resulting in lost business. Financial institutions are compromised by money laundering and other illicit transactions. Their more intimate familiarity with the illicit networks and other discrete elements of the hybrid threat that leech their operations provides them with a far more granular appreciation of the identity, methods, and extent of the hybrid threat. Indeed, the business community has been countering discrete elements of the hybrid threat for some time. Innovative techniques have been developed to counter specific threats and risks, but they are not widely shared. Private sector experience is extremely valuable to NATO in this regard.

experimenting and gaming may provide an atmosphere where issues related to conducting NATO engagement with soft power providers can be explored collaboratively

Assuming NATO decides that engaging the private sector is worthwhile, it must examine ways to ensure that industry is incentivized to respond to the Alliance's outreach attempts favorably. Ideally, industry should be encouraged to reach out to NATO on its own initiative if it believes it is necessary or desirable. To incentivize industry, the Alliance should consider ways to make both outreach and responses to industry engagement transparent and easy. Regular engagement will go a long way toward that end. NATO must also appear to be listening and legitimately seeking input and collaboration. Finally, the Alliance should consider what, if anything, it might provide to industry. On this latter point, recent U.S. experience might be illustrative. Senior command and Department of Defense (DOD) officials regularly engage defense, technology, space, and industry members by providing insights into DOD activities and goals, speeches on leadership, and lessons learned that might be applicable to industry. In exchange, they receive unprecedented access to high-level management and expertise, and even task various private organizations for assistance.

Conclusions

A hybrid threat is more than just the sum total of its constituent parts. Combating such threats does not require new capabilities as much as new partners, new processes, and, above all, new thinking. Experimentation and gaming offer benign, nonhostile forums in which to conduct outreach and to engage civilians where they do not feel threatened. Through the give and take of such activities, both military and civilians may be encouraged to overcome predispositions concerning each other and reach mutual understanding. Civilian participants might make progress toward questioning their prejudices, if any, concerning cooperating with the Alliance.

NATO Allied Command Transformation conducted such an experiment in May 2011 named "Countering Hybrid Threats," during which many of the themes discussed above emerged saliently. The week-long experiment benefited from the participation of nearly 100 private sector professionals, each of whom invested a full working week to the experiment. The number and level of participants and the time they spent suggest that NATO is considered relevant by the business community and that ACT retains an important place in its intellectual leadership. This perception may

pose significant opportunities and a few challenges. It should be noted that a bottom-up approach was used in this experiment, which remains the exception. Taking into account the opinions of experts on the ground can be particularly useful, not only because of their expertise and experience but also because it might prevent us from repeating past mistakes.

Experimenting and gaming may provide an atmosphere where issues related to conducting NATO engagement with soft power providers can be explored collaboratively. While each NATO member may be best suited to engage its own governmental institutions and individuals to find needed capabilities, it is less clear who should approach the private sector. NATO should reach out to large multilateral institutions such as the United Nations, World Bank, and Gulf Cooperation Council to provide the capabilities for the "hold and build" in its most recent deployments. But is institution-to-institution the only desirable engagement? What about engagement of civilians in the preventative or predeployment stage in which NATO might be interested in the knowledge and experience of others in order to shape the environment? What about interactions with nongovernmental and smaller multilateral institutions, including those of the host country or region? At what level should NATO reach out to them and begin to plan cooperatively with a needed civilian workforce? When should it happen? Does it make sense to establish regular relationships with institutions in anticipation of likely problems that NATO may be called on to address in order to shape the environment early? Where should that engagement happen? Is it a function reserved for Brussels and other headquarters elements, or for local commanders as they see fit? Should NATO develop an overarching policy that guides these types of engagements, and what input, if any, should the non-NATO, civilian government, and private players have in developing such a policy?

Synergies among NATO's bodies must be enhanced. That should allow experimentation to impact the ongoing work on the Deterrence and Defence Posture, the Comprehensive Approach, Strategic Planning, and in time, NATO reform. One can hope that this would provide food for thought to the North Atlantic Council in the course of its work during the next few months. It might even allow NATO, with the agreement of member states, to remain ahead of developments and become more proactive rather than remaining reactive. The United Nations, European Union, Organization for Security and Co-operation in Europe, African Union, and others should be engaged, as well as more experts from the diplomatic field.

While NATO member states must lead the way in anticipating the skills, practices, and capabilities needed to confront emerging hybrid threats, the Supreme Allied Commander Transformation and ACT have a vital role in soft power engagement and in initiating a necessary dialogue with those non-NATO actors best positioned to assist in this endeavor. **PRISM**

Notes

[1] *NATO 2020: Assured Security; Dynamic Engagement* (Brussels: NATO Public Diplomacy Division, May 2010), available at <www.nato.int/strategic-concept/expertsreport.pdf>.

[2] Anders Fogh Rasmussen, "NATO After Libya," *Foreign Affairs* (July–August 2011).

[3] Brigadier General Roy Hunstock, Final Plenary, "Military Contribution to Countering Hybrid Threats [MCCHT] Experiment," Tallinn, Estonia, May 13, 2011. This article is based on this experiment, which

was held May 8–13. Further information is available at <https://transnet.act.nato.int/WISE/ACTIPT/JOUIPT/20102011CH/Experiment>.

[4] Fogh Rasmussen.

[5] IMSM-0292-2010, Hybrid threats description and context, May 31, 2010.

[6] Department of Defense Directive 3000.07, "Irregular Warfare," December 1, 2008, available at <www.dtic.mil/whs/directives/corres/pdf/300007p.pdf>.

[7] *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington, DC: The White House, July 2011).

[8] Joint Irregular Warfare Center, "Irregular Adversaries and Hybrid Threats," 2011.

[9] Ibid.

[10] Richard Hills, Opening Plenary, MCCHT Experiment, May 8, 2011.

[11] *NATO 2020*.

[12] Headquarters Supreme Allied Commander Transformation, "Study on Nations' Approaches to Comprehensive Approach," available at <https://transnet.act.nato.int/WISE/ACTIPT/JOUIPT/20102011CH/Experiment/References/StudyonNat/file/_WFS/Study%20on%20Nations%27%20Approaches%20to%20Comprehensive%20Approach%5B1%5D.pdf>.