NEW SECURITY CHALLENGES AND NATO'S FUTURE

Attacks on NATO's governments and their citizens are more likely these days to come in the form of electronic malware through fiber optic cables, or improvised explosive devices in mass transportation systems, or extreme weather conditions disrupting critical energy grids and infrastructure than in the form of tanks and infantry columns crossing NATO's borders… The new security challenges will increasingly test NATO's posture and readiness, whether it is prepared and willing or not. These new threats are good at identifying and exploiting vulnerabilities and they adapt and reorganize very quickly. In the future, no defense will work statically for decades on end as nuclear deterrence and flexible response worked for NATO during the Cold War years. The future belongs to the agile, not to the stolid.

Jamie Shea*

TURKISH POLICY
QUARTERLY

* Jamie Shea is the Deputy Assistant Secretary General for Emerging Security Challenges at NATO Headquarters in Brussels, Belgium.

Since the Berlin Wall came down in November 1989, NATO has not been much involved in the homeland defense business. It has been more visible outside than inside Europe, and has been involved in places that could not be more remote from NATO's Cold War history: Libya, Iraq, Afghanistan and the Gulf of Aden, to name but the most recent examples. Of course, these deployments at strategic distances have been linked to the security of NATO's 800 million citizens at home, according the celebrated phrase of NATO's former Secretary General, George Robertson: "If we do not go to Afghanistan, Afghanistan is going to come to us" (in the form of terrorism, narcotics, refuges and illegal migrants). Yet the validity of this argument depends on NATO's willingness and ability to sustain such a large scale national building operators almost indefinitely. With declining public enthusiasm for these long term, boots on the ground, commitments and mounting pressures on defense budgets, this will not be possible in the future. If NATO will no longer be primarily defending its populations abroad, it will need to do it increasingly at home, and be more visible in what the U.S. has termed the "Homeland Defense."

This also comes from a recognition that attacks on NATO's governments and their citizens are more likely these days to come in the form of electronic malware through fiber optic cables, or improvised explosive devices in mass transportation systems, or extreme weather conditions disrupting critical energy grids and infrastructure than in the form of tanks and infantry columns crossing NATO's borders.

These are not only the most likely threats; they are also the ones that our citizens are most worried about, especially as they see how easy it is in modern societies for disgruntled individuals to access software programmes free on the internet to steal our credit cards and personal data, or to build rudimentary explosives in their home kitchens. In short, if the vulnerability of the information technologies, energy grids, and mass transportation systems, on which we all increasingly depend on, is now the main security threat, NATO has to widen its remit to bring these new challenges under its traditional notion of collective defense and solidarity. Otherwise, there is the danger that when NATO's ISAF mission ends in 2014 (and other operations in Kosovo, Bosnia, the Gulf of Aden and Libya wind down as well), the Alliance will lack a significant transatlantic security project to maintain its recent high profile, and to mobilize the resources and political energy of its member nations.

For these reasons, it was not surprising that NATO's new Strategic Concept, adopted at the Lisbon Summit in November 2010, gave the new security challenges a central place. Terrorism, cyber attacks, the proliferation of weapons of mass destruction, energy vulnerabilities and environmental constraints were highlighted in particular. This was not so because they cover all the new threats (for instance pandemics or organized crime were not mentioned) but because these are the areas where NATO's essential military capabilities have some value to add to broader international efforts. In addition, the Strategic Concept also calls on NATO to monitor and analyze the international environment in order to anticipate crises as a first step to better preventing them. It is estimated, as a result of a research conducted by Brown University in the United States, that the U.S. has, thus far, expended 3.7 trillion dollars in responding to the 9/11 attacks. Half of this sum has gone on the U.S. deployments in Iraq and Afghanistan. Overall, this expenditure represents no less that 25 percent of the U.S. national debt. Clearly, security is not going to be a "budget neutral" activity for a very long time, if ever again. So, prevention and using more political instruments to manage crises, particularly in their early stages, will no longer be simply desirable but essential.

This said, in adopting the new security challenges, NATO was not just adding to its shopping list. It was also presenting itself with a number of cultural, organisational and conceptual challenges. First and foremost, this is because with the exception of ballistic missile and WMD proliferation, the new challenges are largely civilian. Eighty percent of the internet is privately owned and there is no national jurisdiction or 200 mile territorial limits in cyber space. So, the new challenges can not be confronted through the mathematical construction of a set of military forces or by the threat of military retaliation. Moreover, these challenges may not engage collective NATO defense and solidarity as easily or as automatically as a Soviet tank thrust through the Fulda Gup in the Cold War days. Only one ally may be affected by an energy cut-off, or a cyber or terrorist attack. What is the threshold for activating NATO's Article 5 if a country is paralyzed for days but no equipment is permanently damaged and nobody is physically harmed? In this case, would NATO solidarity not apply more to helping that affected country to limit the damage and recover than to going to war on its behalf? Or, alternatively, would solidarity not apply more to trying to prevent these attacks in the first place, or denying the attacker any benefit, than to responding collectively and with massive force after the event?

> *"…prevention and using more political instruments to manage crises, particularly in their early stages, will no longer be simply desirable but essential."*

In sum, meeting the new security challenges will require NATO to adopt a new business model. Rather than relying only on deterrence and defense to ward off threats from actors that will likely be more often than not non-state groups or lone individuals, NATO will have to operate on the principle that attacks by these non-state actors (many of them are anonymous) will inevitably happen. Security policy must, therefore, be to make them harder to carry out and less successful – and with a higher degree of ability to attribute the sources of the attack via forensics and freezing of the evidence. So, Allies have to develop a real understanding of how cyber space operates (as opposed to the more familiar notions of air, sea and land space): they must step up intelligence cooperation on these threats and identify the critical infrastructure (whether IT pipelines or grids) that needs to be protected. They must also better grasp the nature of hybrid threats. For instance, environmental decay and illegal industrial waste dumping off the coast of Somalia leads to a decline in fish stocks; Somali fishermen then resort to piracy which in turn drives up insurance premiums for international shipping and leads to an expensive deployment of counter-piracy warships; the ransoms for the pirated vessels are taxed by the local extremist organization, Al Shabab, which uses the proceeds to buy arms and plan attacks, including hostage taking in neighbouring Kenya; this leads to hostilities between Kenya and Somalia and to a Kenyan incursion into Somali territory, provoking regional tensions. NATO has to not only understand the threats individually but also analyze how they impact on each other to turn a local threat into potentially a major international headache.

> *“[NATO] has to accept to be a part of the chorus rather than the leading tenor or soprano.”*

NATO’s new approach must focus on prevention, recovery and overall resilience. Yet this involves a second cultural shift. The NATO of the past was an alliance that had, generally speaking, an “all or nothing” approach. Either the alliance owned the issue almost entirely, being by far the principal actor, or it stayed on the sidelines. Think of Bosnia, Kosovo, Afghanistan or Libya. NATO’s involvement and contribution were significantly greater than for any other actor, and for large portions of the campaigns. Missile Defense is another area where NATO is totally in the lead in what is exclusively a military programme. Yet the great majority of crises involve a very broad spectrum of actors and assets (police, intelligence services, emergency rescue agencies, the private sector, citizens action groups, Interior Ministries and other international organizations). There are currently over 30 different international agreements and codes of conduct in the area of cyber security – and many more in the pipeline. NATO can add valuable capabilities and expertise in areas such as cyber, critical infrastructure protection or counter-terrorism detection technology but it cannot play the dominant role. It has to accept to be a part of the chorus rather than the leading tenor or soprano. That means defining policies that not only support NATO's own requirements but support the efforts of others and fit into an established international framework of norms and cooperation (for instance, making NATO's use of cyber defense or emerging technologies fit in with international humanitarian law or the laws of armed conflicts). Moreover, if NATO is to develop its niche areas, it will need to interact more with the branches of the governments that have the main responsibility; for instance, Interior Ministries, cabinet offices, intelligence services, police and Interpol and Europol. When NATO HQ organized a meeting of the national heads of cyber defense earlier this year, a large number of the participants had never been to NATO before. So, NATO will need to be able to reach beyond its traditional stakeholders in the Foreign and Defense Ministries and create a new operational and consultative network. Will the Foreign and Defense Ministries agree to share "NATO power" with their Interior Ministry or police counterparts? Will the latter see NATO, with its heavily military culture, as a visible interlocutor? Will NATO be able to run successful partnerships with industry in areas such as intelligent software, malware detection, internet identification smart grids or new counter terrorism technologies so as to steer industry towards NATO's needs? This is the key challenge.

The creation of a new division (Emerging Security Challenges) in the NATO International staff in August 2010 has given this new area of NATO's work a distinct focal point. The new division has been able to bring the rather fragmented strands of NATO's previous efforts together in a more coherent whole, and, then, increasingly join those efforts up to the work of other bodies such as the UN, OSCE, EU, and Council of Europe. It has also carried out a review of all of its activities to cut down on duplication of effort and to steer them towards NATO's key priorities rather than as ends in themselves. The partner dimension has also become increasingly important. Last May, NATO Foreign Ministers in Berlin offered the partners an upgraded relationship based on an expanded toolbox of cooperative activities and more "28+N" consultations with those partners that have specialist expertise and resources to contribute. Many partners share a common vulnerability and interest in dealing with the new challenges alongside the Allies (perhaps more than in contributing to out of area deployments). Consequently, outside interest in working with the division is high and despite some political obstacles (such as the sharing of sensitive intelligence on cyber threats and methodologies), NATO must build new coalitions with partners. It is also a way for Europe and North America to push their norms (for instance on a cyber code of conduct or confidence building measures) within the broader international community.

Over the past year, NATO has chalked up some successes in expanding its role on the new security challenges. It has agreed a new cyber defense policy and related action plan. These will bring NATO's own networks under a centralized, 24/7 cyber management while allowing the alliance to provide more immediate and longer-term assistance to its members in areas such as training, education, systems configuration, intrusion detection and consequence management. Two rapid response teams are being established and the NATO Center of Excellence on Cyber Defense in Tallinn, Estonia is conducting exercises and pooling information and expertise. Cyber defense is gradually being incorporated into NATO's defense planning and NATO exercises are rehearsing the procedures and decision making cycles for assessing and reacting to cyber attacks. NATO is also conducting an in-depth review of the political and military instruments to combat terrorism that it has employed since 9/11. It is also revising its Defense against Terrorism Programme of Work to look at training and process management as well as at hard core capabilities such as force protection and helicopter and aircraft survivability. The needs of Special Forces, especially in the area of forensics, are becoming more important. NATO's approach to energy and environmental security is also becoming more systematic, especially in the area of critical infrastructure protection where we can build on much previous work in the field of civil emergency planning and established best practices exchanges between government and the private sector. At the same time, the alliance's new strategic analysis capability has helped the NATO Ambassadors to consult on real or potential crisis areas, to improve their situational awareness, and to identify how NATO's many tools (partnerships, training programmes, more integrated civilian – military planning, rapid response forces) can be better used for crisis prevention and management – rather than being mobilized only late in the day when the crisis has turned into a full-blown conflict.

"In the future, no defense will work statically for decades on end as nuclear deterrence and flexible response worked for NATO during the Cold War years."

So, the record after one year is a respectable one: but it is not yet fully satisfactory. NATO will need to develop the high level political attention and the holistic approach needed to respond effectively to the emerging threats. It cannot wait for the next energy crisis or Estonian-type cyber attack to get its act together. These challenges are the future of collective defense. Inevitably, over the past years, dealing with NATO's operations has taken up the greater part of the alliance's time, at the expense of discussing other equally pressing challenges, unless, of course, they dovetail with operational requirements, such as the need to develop technology to counter the terrorist use of improvised explosive devices in Afghanistan. Also, some alliance countries have been sceptical of NATO's legitimate role or added value in dealing with these challenges believing that the response lies primarily with other bodies, such as the UN or EU, even though these bodies are often keen to cooperate with NATO and acknowledge its expertise in key niche areas. Such concerns can only be dispelled if the allies devote more time to discussing the new challenges and to agreeing coherent NATO policies that allow the NATO military and civilian staff to work more freely in areas where NATO's expertise and added value are proven.

Trotsky famously said: "you may not like war, but war likes you." Similarly, the new security challenges will increasingly test NATO's posture and readiness, whether it is prepared and willing or not. These new threats are good at identifying and exploiting vulnerabilities and they adapt and reorganize very quickly. In the future, no defense will work statically for decades on end as nuclear deterrence and flexible response worked for NATO during the Cold War years. The future belongs to the agile, not to the stolid. So, the new emerging threats will force their way onto NATO's agenda. It is better, then, that we are prepared to face them before they face us.