How is NATO Dealing with Emerging Security Challenges?

By Jamie Shea

The views expressed in this article are those of the author alone. They do not represent an official position of NATO.

For most of human history, states have seen their primary role in the field of security as the defence of their borders and their territories against the predations of other states. Though populations faced other threats, such as famine, major epidemics or starvation, governments felt no need to intervene unless there was an immediate threat to the state or social order.

Today, states have taken on the responsibility to cope with a much broader spectrum of threats because of, voters' increased expectations of protection and globalization, which has made states much more vulnerable to non-traditional security threats. These can be easily transmitted across borders and can originate virtually everywhere: local and international terrorism, cyber threats to public and private networks, the spread of diseases and pandemics, vulnerabilities to critical infrastructure and energy grids, dependency on globalized supply chains, extreme weather conditions, uncontrolled immigration, organized criminal networks, and the proliferation of chemical, biological, radiological and nuclear (CBRN) devices with greater use of delivery vehicles such as missiles. The national security strategies of most NATO countries today prioritize these non-traditional threats before the more traditional threats from rising and rival powers or collapsing states. Although most of these non-traditional threats have existed for some time, NATO has only recently focused its attention on them.[1]

However, the Alliance is still associated with more classical military operations that take place outside its territory and emphasize flexible and deployable forces capable of cooperating with non-governmental organizations (NGOs), election observers, police trainers and democratic institution builders.

The "Responsibility to Protect" is partly responsible for NATO's shift away from the defence of states to the defence of populations. Simultaneously, NATO linked its interventions to traditional security interests.[2] Thus, despite the frequent portrayal of interventions as part and parcel of a new international morality to uphold human rights in foreign lands, in reality NATO has not strayed far from its traditional focus on the security of its member states.

Given this focus on defending and protecting interests, NATO has recently had to consider the new spectrum of threats which are not classically military in nature but which will undoubtedly be frequent sources of disruption in the years ahead. Moreover, these threats can originate just as easily from within our borders as from outside. Malicious individuals may easily gain access to modern technologies (int. al. malware, drones, robotics and bioengineering), giving them the disruptive power that used to be the preserve of states. We could live in a future in which anyone could be targeted, anywhere, and at any time. These non-conventional threats cannot be deterred by the threat of military retaliation in the way that nuclear weapons could maintain a balance of power and peace, albeit uneasy, throughout the Cold War. Cyber attacks, for instance, have been a daily occurrence almost everywhere and most can still be carried out with relative impunity. The gain from espionage or financial crime greatly outweighs the risk of being caught or even the current legal penalties. Thus there is yet no significant incentives for the attackers to desist other than that they may damage and degrade information and communications infrastructure on which they also depend. It would be good if this “deterrence through interdependence” would eventually take hold, but we are clearly still a long way from it.

Deterrence or Prevention.

Similarly, regarding terrorism, an attack by suicidal fanatics is difficult to pinpoint in advance or to stop, as we do not have the means or even the social ambition to permanently defend every conceivable vulnerability to our economies and societies. Too much protection would constrain people's liberties and freedom of movement and seriously undermine the way of life that NATO defends. Furthermore, a terrorist who accepts death as the inevitable outcome of his mission is not amenable to deterrence but only prevention. Consequently the early warning systems and methodologies that NATO relies upon to underpin deterrence or even to mobilize its own resources in anticipation of an attack no longer work. The best it can do is to achieve some early warning of an attack, calculate how to best limit the damage and recover as quickly as possible.

Attribution and Retaliation.

Another problem is attribution. Actors come in ever smaller groups or use modern technologies, such as encryption, to cover their tracks. A cyber attack can be routed through so many countries that it is difficult to trace and can be started by an individual in a location remote from himself. A terrorist cell can operate thousands of miles away from its directing headquarters (HQ). Establishing proof of culpability, especially in the event of cyber or terrorist attacks, can take a long time. In some cases, such as cyber attacks, a response has to come within nano seconds to prevent further penetration of a network and major damage. This rapidity of response does not always fit organizations such as NATO, which is best at orchestrating military responses and often needs lengthy consultations to build consensus and to approve detailed operational plans and rules of engagement before acting. A military response may also not be the right response; for instance after an energy cut-off or a terrorist attack. If we have clear evidence that a state and a single leader is responsible, then a military operation is appropriate, but most modern attacks do not fit this "singe aggressor" paradigm.

What level of solidarity can we expect and can we offer?

These threats are not existential in the way that a Soviet tank thrust through the Fulda Gap or a rocket strike would have been for all Allies during the Cold War. No lives were lost or critical infrastructure damaged when Estonia suffered a devastating eleven-day distributed denial of service (DDoS) attack in 2007. The situation in the twenty-five other NATO member states at the time remained quite normal. What is the threshold for a collective response? Some Allies believe that a response should be collective and multinational from the outset. Others believe that the nation is primarily responsible, for instance in the protection of critical information or energy infrastructure. NATO's entire history has been dedicated to fostering a collective approach to security and promoting the primacy of collective responses. But cyber defence is an area where we have largely gone back to national policies and programmes; nations are still very secretive even vis-à-vis their Allies regarding their cyber vulnerabilities or cyber capabilities and reluctant to share information beyond the very small trusted communities in which their intelligence services and private-public partnerships operate. It would thus take some time and effort to raise cyber defence within NATO to the same level of collective engagement as traditional force planning or force generation for operations. It took NATO many decades to persuade its members to adopt a collective approach and to share their capabilities and defence plans, recognizing that in this way they would ultimately have more security. In dealing with new challenges like cyber threats, however, we cannot afford the luxury of several more decades before we arrive at the same collective approach.

The proliferation of actors.

A final challenge is the fact that most of the non-traditional threats require responses by various actors and here NATO is rarely in the lead - a culture change for the Alliance, which for sixty years has been a leader in its field. NATO is not accustomed to sharing leadership and decision-making responsibilities with a range of different civilian actors outside the conventional military chain of command. Cyber issues require links with interior ministries, intelligence services, the police and cabinet offices that are not NATO's normal interlocutors and have no permanent bureaucratic links with NATO HQ of the sort that foreign and defence ministries have long enjoyed. Moreover, as over ninety per cent of information networks are owned by the private sector, the ability to bring private companies in to everyday cyber defence management is crucial to success. NATO no longer defines the terms. Allies may be reluctant to be told by private industry what the threat is and to have to share daily management after decades of seeing industry purely as the deliverer of a capability decided uniquely by governments. But this is already happening at the national level in the cyber area and in information and intelligence sharing, and it will have to be elevated to the international level as well.

NATO's Responses.

Consequently, NATO's traditional toolbox of political consultation processes and military means can be useful in addressing the new security challenges but it is certainly insufficient for serious action. To have a real impact rather than simply raising awareness about the new threats NATO has to be willing to adopt measures that fall outside the traditional mould of high-end conventional military conflicts. The nature of the challenges has to define the responses. Also, NATO has to be honest in admitting that it has no "silver bullet" and that in some areas its role will be subjugated to other actors. For instance, missile defence is an exclusively military programme where only one Ally, the United States, has the radars, missile interceptors and overall systems architecture to provide the capability to the Alliance. The other Allies may have elements that they can add on (for instance, Patriot air defence missiles or satellite and reconnaissance assets) but they cannot replace the US in this area. Other issues, such as cyber, terrorism and energy security are very different. Here the non-US Allies have very important capabilities but many of these are in the civilian area (for instance intelligence). NATO would thus not be the only or even the principal forum of activity. Consequently the Alliance has to define carefully the areas where it can add value to the existing international efforts to contain and counter these new threats. The overall challenge is to avoid promising more than it can deliver; but, at the same time, not to become so reductionist or minimalist that NATO ends up leaving its member states vulnerable in areas where it is perfectly capable of protecting them.

What does this mean in practice?

The first step is to create a clear mandate for the Alliance to deal with these challenges. This was accomplished in the new NATO Strategic Concept[3] and Lisbon Summit Declaration of 2010[4], which placed cyber, terrorism, energy security and CBRN threats on the same priority level as more traditional threats such as state aggression. Certainly the eloquent language of these high-level political statements does not in itself guarantee full consensus among the Allies on its interpretation, nor the implementation. But it is the necessary beginning.

The second step is to create a firm bureaucratic foothold in the NATO organization. The recently established Emerging Security Challenges Division (ESC) within NATO today brings the following threats under one roof: Cyber Defence, Counter-Terrorism, Energy Security, WMD Proliferation and Nuclear Policy, Strategic and Defence Economic Analysis and Scientific and Technological Cooperation with NATO's multiple partner countries. The new unified division facilitates tackling the crosscutting nature of the challenges. They are frequently most ominous in a combination thus achieving a critical destructive or disruptive mass; for instance terrorist attacks on critical infrastructure, cyber attacks on supervisory control and data acquisition systems (SCADAs) that control energy pipelines and electricity grids or terrorist access to weapons of mass destruction and associated missile technologies. Given NATO's continuing preoccupation with its operation in Afghanistan and the consequences of defence budget cuts in North America and in Europe for the future levels and interoperability of its armed forces, a single ESC Division helps to keep these issues on NATO's agenda. It supports Allies in focusing on cost-effective prevention and resilience measures, even if there has not been (thankfully) a major terrorist strike or a paralyzing cyber attack in many NATO countries for some years to galvanize political attention and mobilize resources.

The third step is to develop coherent policies in all these areas with a common denominator that the Allies are all willing to support. This establishes the political and technical basis needed for the Allies to be more willing to agree to concrete actions in the subsequent implementation plan. Since its establishment two years ago the ESC Division has updated NATO's policy documents in all the key areas. It has developed a cyber policy and action plan; new counter-terrorism policy guidelines and work is on-going on an associated action plan. After difficult debates, Allies now have a clearer view on how NATO can contribute to energy security, particularly in the realm of critical infrastructure protection and a sharing of best practices among government and industry experts. NATO has also reviewed its WMD arms control and nuclear policies and has developed a new doctrine for defence against CRBN devices. Its Science for Peace and Security Programme (SPS) is now more focused on key priorities which link science and technology to NATO's core activities making it more relevant to Allies. One example is a project that led to the emplacement of scanners at the borders of Central Asian countries and Afghanistan. These scanners improve the customs of our partner countries and facilitates the transit of military equipment coming in and out of Afghanistan in support of NATO's ISAF mission. NATO has also come to the conclusion that it has to be able to identify threats more in advance and be less reactive. This can be done by establishing the link between threats at an earlier stage (for instance, weapons, transfers, organized crime and terrorism in the Sahel region) and identifying the triggers that can mark their evolution from a local problem to a real security threat to NATO. This also generates periodical attention by identifying various scenarios and the pros and cons of different courses of action by NATO – from early to late. A Strategic Analysis Capability and an Economics Assessment Unit are helping to spark discussion and inform decisions regarding these future crisis areas and the means NATO has to respond. This type of staff work unfortunately does not guarantee political attention but without it political consultations would not happen or produce any actionable conclusions.

The challenge now is to build capabilities.

NATO has always been an organization based on physical capabilities, such as integrated command structures, common communications and planning mechanisms, and forces. Thus, the new challenges will be more effectively anchored in the Alliance if they also have a hard capability dimension. In cyber defence, this currently means upgrading the NATO Computer Incident Response Capability[5] to allow it to protect NATO's civilian as well as military networks and to have the most advanced assets for detecting intrusions, freezing data for analysis and evidence, and sending rapid response teams to assist Allies facing cyber attacks. For the first time this year, cyber defence will become part of NATO's defence planning process and nations will accept Capability Targets to create more effective national cyber defence organizations and national Computer Emergency Response Teams (CERTs) to centralize cyber defence management and responses. In the field of terrorism, NATO is developing technologies to detect suicide bombers (the Stand-off Detection of Explosives - STANDEX project) and counter improvised explosive devices (IEDs). These may have originated from operational requirements in Afghanistan but they will be useful in other operations and also in civil defence at home. In energy security, NATO has developed best practices on protecting critical infrastructure and has a project to enhance the more efficient use of energy in the military, given our recent experience of having to transport fuel to Afghanistan at very high cost.

Building on these activities, NATO has been trying to factor the emerging challenges into its exercises. Handling a cyber crisis is not the same as handling a conventional or WMD attack. Exercises are useful to identify and fix the weaker spots in NATO's political procedures and military capabilities and to discern issues that may not always surface in normal political consultations. They not only pinpoint institutional weaknesses but also expose national positions and disagreements, which can be hidden in more theoretical debates. Exercises are also a good way of obliging nations to clarify, which capabilities they are prepared to make available to NATO in a crisis and how ready for use those capabilities are.

Highly networked challenges require highly networked responses.

We have long spoken of the need for a comprehensive approach to military operations, where military and civilian efforts are integrated from the outset, but we need this comprehensive approach just as much in dealing with cyber attacks, terrorism or energy cut-offs. As we know in this field, many branches of government as well as the private sector are involved. The Dutch Cyber Defence Information Centre has no fewer than fourteen government agencies permanently participating, all of whom would be expected to be involved in managing a major cyber attack. So it is important to have clear procedures, validated through exercises to determine the respective roles of all key actors, thereby avoiding duplication, gaps or mutual blockages once a crisis occurs. As NATO lacks early warning regarding specific attacks, it also becomes all the more important to improve the overall understanding how these threats originate and to chart their evolution, both geographically and functionally. NATO needs to determine at which point of the threat chain a NATO response is both justified and effective. The challenge is to identify the right point for counter-measures against threats such as cyber or terrorist attacks. This also includes summoning the political will to act timely and decisively against these threats before it is too late and our societies are severely harmed.

It does not have to be a choice between a full-scale NATO military intervention or no involvement at all. To be successful, NATO must appeal to and build closer ties with other international organizations, NGOs, think-tanks and the private sector. For the first time in its history, NATO is dealing with challenges that cannot be understood and responded to within the narrow confines of its own twenty-eight members. NATO must also embrace its partner countries that share the urgency of the threat and have as much to contribute as to receive in terms of intelligence sharing and experience. Post-ISAF, partners may well become less involved in NATO's operations; thus it becomes all the more important to sustain these partnerships by anchoring them also in the emerging security challenges. The Alliance will have to become as good at leveraging the contributions of others as in inducing its own members to act. If the future of security for the Western countries is to do less themselves and rely more on the local actors, then organisations like NATO will have to improve their political dialogue with the new African, Asian and Arab security actors in order to foster more genuine trust.

In conclusion, dealing with the new challenges requires NATO to take a less reactive and more anticipatory approach. We cannot restrict our discussions only to the immediate crises. NATO will have to consider a much broader intellectual landscape and identify multiple niche opportunities where NATO can make a difference. This will require a change of mind-set and more focus on what other actors are doing in the field of international security so that NATO has a better understanding of the strengths and weaknesses of their operations should it be called upon to support them. Modern security challenges are much more multifaceted and complicated than what we have seen in the past. Complexity could in itself become a form of self-deterrence if we start to believe that we should not try to influence regional conflicts or crises because we do not sufficiently understand the actors on the ground or the dynamics at play. Our publics might be relieved that less engagement means less cost or risk, particularly after Iraq, Afghanistan and Libya; but to let the rest of the world go its own way and to remain on the side-lines looking outwards cautiously is not a long-term recipe for stability in the 21st Century. Therefore NATO will have to ensure that its actions are based on the best and most detailed knowledge of the security environment around it, particularly in an age where defence budgets will be subject to the same stringency as every other government spending programme and the margin for policy errors or waste of precious resources are far narrower.

In sum, addressing the new security threats is a daunting challenge for the Alliance. It will have to become a hub of political dialogue and security services rather than a monolithic structure focussing only on one security issue at any given time. As this article has demonstrated, some significant cultural and intellectual changes are required but the Alliance has also many of the standard ingredients for success: a record of adaptability, a large range of willing and able partners, legitimacy in the UN and more broadly and, last but not least, its proven military planning and capability development structures. So although the challenge to remain relevant is daunting, it is also entirely manageable.

[1] Even the first cyber attack (allegedly against a Soviet pipeline in Siberia) goes back to 1983.

[2] For instance, the interventions in the Balkans in 1995 and 1999 were justified by the need to prevent a spill over of the conflict onto NATO territory. The overall objective of the International Security Assistance Force (ISAF) in Afghanistan remains the stabilization of Afghanistan in order to prevent the country from re-emerging as a base for terrorist attacks again NATO Allies. For reference see The North Atlantic Treaty Organization, The North Atlantic Treaty, 4 April 1949.

[3] NATO’s New Strategic Concept, North Atlantic Treaty Organization, Accessed March 17, 2013, http://www.nato.int/strategic-concept/index.html.

[4] North Atlantic Treaty Organization, "Lisbon Summit Declaration", 20 November 2010, Internet, http://www.nato.int/cps/en/natolive/official_texts_68828.htm.

[5] North Atlantic Treaty Organization, NATO and Cyber Defence http://www.nato.int/cps/en/natolive/topics_78170.htm.