



NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm

Michael Rühle

ABSTRACT New security challenges, ranging from cyberattacks to failing states, cannot be deterred by the threat of military retaliation, nor will military operations be the appropriate response in most cases. Instead, the emphasis must be on prevention and enhancing resilience. If the North Atlantic Treaty Organization (NATO) wants to play a meaningful role in addressing such challenges, it will have to develop a clearer understanding of the nature of these challenges, build closer ties with other nations and institutions, and seek partnerships with the private sector. Above all, allies will have to use NATO as a forum for discussing emerging security challenges and their implications.

KEYWORDS cyberattacks; energy security; NATO; strategic concept; terrorism

On April 27, 2007, Estonia became the victim of a major cyberattack. Over a period of three weeks, the servers of the Parliament, ministries, banks, and media of the small Baltic North Atlantic Treaty Organization (NATO) member were disrupted or paralyzed by an attack that utilized servers in more than 100 countries. Six years after the assault on New York and Washington, when a group of terrorists guided from Afghanistan had managed to launch a strategic strike against the world's strongest military power by using entirely non-military means, NATO's cyberexperts experienced their very own "9/11."

However, unlike on September 11, 2001, the attacks on Estonia did not lead to the invocation of the Washington Treaty's collective defense clause, nor was there a military operation against the presumed perpetrators. The model of Afghanistan was not applicable to an anonymous cyberattack. Neither deterrence nor retaliation proved to be useful categories. Only one option remained: in future, the electronic infrastructure of allies would have to be hardened to the point where such attacks would not cause too much damage.

The steady increase of cyberattacks worldwide demonstrate that what happened in Estonia in 2007 was no singular event. Nor are cyberattacks the only security challenge that cannot be deterred by the threat of military retaliation. Terrorism, cyberattacks, "failed states," the proliferation of weapons of mass destruction, the increasing vulnerability of energy and raw material supply, and humanitarian disasters are developments that lie

Michael Rühle is Head of the Energy Security Section in NATO's Emerging Security Challenges Division. Previously, he was Deputy Head of the Secretary General's Policy Planning Unit. He has published frequently on transatlantic security issues. The views expressed in this article are the author's own.

beyond the deterrence paradigm. Nor will military operations constitute an appropriate response in most circumstances. The real answers to these non-traditional challenges lie beyond deterrence and retaliation: they lie in prevention and enhancing resilience. For NATO, which seeks to safeguard the security of almost 900 million citizens, this means a significant change in the way it thinks and acts.

FROM GEOGRAPHICAL TO FUNCTIONAL SECURITY

The inadequacy of a passive, retaliation-based approach has been realized since the end of the cold war. That period's specific characteristics—a single, visible enemy, symmetrical military capabilities, long warning times and, above all, the assumption that the opponents would be guided by a rational cost-benefit calculus—made nuclear deterrence a congenial (and affordable) means of war prevention. These characteristics have long disappeared. NATO's unsuccessful initial attempts to exert a moderating influence over the conflicts resulting from Yugoslavia's disintegration in the early 1990s were a strong reminder about the need for a different approach. A policy that for over 40 years had been centered around the mere display of force did not provide any useful options in a conflict between third parties. The conflicts in the Western Balkans could only be stopped by a military intervention.

NATO's military engagement in the Western Balkans, which helped end the conflicts in this region and provided the secure environment for a fresh start, was the first indication of a shift toward a more active approach. Given the novel character of this mission for NATO and its potential implications for Europe in general and the Alliance's future role in particular, the decision to become engaged had only come about after long and painful debates among allies. However, the decision to intervene in Afghanistan after the terrorist attacks of "9/11" was taken almost instantaneously, without lengthy debates. The "out-of-area syndrome" that had prevented NATO from contemplating military action outside the NATO Treaty area had finally been shed.

Yet even the post-"9/11" change from a geographical to a functional understanding of security will not be sufficient for NATO to meet the challenges of the early twenty-first century. On the one

hand, the many problems of the Afghanistan mission reveal that the high price of major military engagements will be paid only in the most serious of circumstances. On the other hand, the relationship between a specific terrorist act and a "failed state" will hardly ever be as clear as it was in the case of the link between "9/11" and Afghanistan. Hence, while the preparedness to intervene militarily without geographical restrictions is indispensable for any meaningful security policy in the globalization age, it is not sufficient for addressing the full spectrum of risks and threats.

THE EMERGING SECURITY ENVIRONMENT

A look at the emerging security environment substantiates this assertion. According to mainstream analysis, the coming decades will see a decline in state sovereignty, a power shift from states to international or non-state networks, and an increase in the destructive power of these non-state actors. Another important development is the continued reliance on civilian nuclear power generation. In addition to its technical safety challenges, the use of nuclear energy could pose significant risks of military nuclear proliferation. At a minimum, it will lead to an increase in the number of "virtual" nuclear weapons states, capable of converting their civilian programs into military ones at short notice. As NATO's 2010 Strategic Concept notes, "[d]uring the next decade, proliferation will be most acute in some of the world's most volatile regions."

Another characteristic of the emerging security environment is the continuing phenomenon of "failing states." As many of these ungoverned spaces may become a training ground for terrorist groups or a safe haven for pirates and drug and people traffickers, the security implications of these states' "failure" will reach far beyond their place of origin. Cyberattacks, which have already become a new form of permanent low-level warfare, will further increase in frequency and sophistication, moving from the disruption of services to the outright destruction of hardware. Energy security will also become an increasing concern. As the Strategic Concept puts it, "[s]ome NATO countries will become more dependent on foreign energy suppliers and in some cases, on foreign energy supply and distribution networks

for their energy needs. As a larger share of world consumption is transported across the globe, energy supplies are increasingly exposed to disruption.”

These developments may be aggravated by other political and environmental changes. One such change is the emergence of new global players, which may not always want to play by rules that they view as having been largely developed by—and serving the interests of—the West. Another spoiler might be climate change, which may not only lead to an increase in natural disasters but also raise other challenges ranging from food security to pandemics.

TOWARD PREVENTION AND RESILIENCE

While this picture is far from complete, it demonstrates why a deterrence-based approach will not suffice if NATO is to play a meaningful role in this new security environment. For example, terrorist attacks in a subway or an airplane cannot be prevented by the threat of military retaliation but only by police and intelligence cooperation. By the same token, the frequently discussed scenario of a terrorist “dirty bomb” causing panic by spreading radioactive material is also beyond the classical logic of deterrence. By contrast, the fact that since “9/11” many terrorist attacks were thwarted by police and intelligence cooperation emphasizes the preventive dimension of current security policy. New technologies that would help to detect explosives or to trace their origin will therefore gain in importance. The same applies for measures to limit the damage after a successful terrorist attack. Again, the classical paradigms of deterrence and retaliation do not apply, nor will military operations constitute the appropriate response.

The same logic applies to attacks against critical energy infrastructure. Whether it is terrorist attacks against pipelines or cyberattacks on power networks: deterrence by the threat of military retaliation is as irrelevant as is a military operation against the (mostly anonymous) perpetrators. As with cyberdefense, the key to security lies in the resilience of the infrastructure itself: redundancies make it possible to ensure the uninterrupted flow of oil and gas, the rapid repair of the damaged pipelines can keep the losses within acceptable limits, and the

electronic systems in control centers must be designed in such a way as to “ride out” even a sophisticated cyberattack.

The principle of damage limitation is also going to gain in importance with respect to the proliferation of weapons of mass destruction. As globalization has opened new possibilities for the transfer of knowledge and technology, the number of states with nuclear, biological or chemical weapons might increase. This could lead to a constellation of deterrence relationships that has little in common with the bipolar nuclear standoff of the cold war. The logic of deterrence by the threat of punishment will remain indispensable for inducing military restraint among states, which is why NATO has declared that it will remain a nuclear Alliance as long as nuclear weapons exist. However, a deterrence system that features multiple stakeholders will be more fragile, as the lack of transparency and predictability will make such a system more prone to technical failure and political miscalculations. Again, the focus must be increasingly on prevention and resilience: prevention through an active non-proliferation policy, export controls and sanctions; resilience through new defensive measures such as the establishment of a NATO-wide missile defense.

The last example of the paradigm shift is humanitarian relief operations. It has by now become a general consensus that climate change is a reality, that it is irreversible, and that it will have serious security implications. While climate change is a global phenomenon, its most dire consequences will reveal themselves particularly in those regions that are already at a disadvantage and thus do not have the means to protect themselves. The predictable result of these developments will be an increase in natural disasters, civil emergencies, and, consequently, in humanitarian relief operations. Since the military is best equipped for these missions it will often be used a “first responder” in such emergencies. The use of the military in such operations has nothing in common with traditional warfare, however, as the aim is not to impose one’s political will on an opponent but rather to ensure that the aid reaches the victims. Put another way, the issue at stake is not how to deter a threat but how to mitigate the negative consequences of events that lie beyond human control.

A SENSIBLE NATO AGENDA

As an Alliance that seeks to safeguard the security and well being of almost 900 million citizens from 28 nations, it is indispensable that NATO adapt its policies in line with the ongoing paradigm shift. This should not be misunderstood as a move away from operations such as in Kosovo, Afghanistan, or Libya: collective military operations are likely to remain the core business of NATO, as this is the area where the Alliance offers its most significant added value. However, the dimensions of prevention and resilience will have to occupy a much more prominent place on NATO's political and military agenda. Such an agenda must be built around several key elements.

First, NATO needs to develop coherent policies to define its role in addressing the emerging security challenges mentioned above. NATO has been addressing a range of emerging threats for quite some time, yet it has done so in a compartmentalized way, without clear-cut political guidance or a thorough conceptual underpinning. The 2010 Strategic Concept, which gives considerable prominence to emerging challenges, signals a change, however, as it provides NATO with a wide-ranging mandate to address these challenges in a more systematic way. Moreover, the creation of the Emerging Security Challenges Division in NATO's International Staff will facilitate a more coherent policy development and implementation in these areas. A first result of these developments was the agreement on a NATO Cyber Defense Policy, which aims at introducing NATO-wide standards to protect against cyberattacks, and at integrating cyberdefense into the NATO defense planning process. Another indication of a more coherent NATO policy with respect to emerging security challenges is the decision to build an Alliance-wide missile defense system, preferably in coordination with Russia.

These steps now need to be mirrored in other areas. For example, ongoing counterterrorism measures, such as naval patrols in the Mediterranean or the development of sensors to detect suicide bombers in subways, should ideally be embedded in a comprehensive NATO counterterrorism policy. NATO's approach to energy security, which currently focuses predominantly on critical infrastructure protection, could gradually be expanded, for example

by making greater use of NATO's training and education facilities and by a particular focus on enhancing fuel efficiency in military operations. Regarding environmental security, there is a need for a more systematic networking with the scientific community to identify technical and scientific trends.

Second, NATO needs to be much better connected to the broader international community. This is true for its relations with other security stakeholders such as the European Union, the United Nations or numerous nongovernmental organizations (NGOs), but also for its relations with other countries, notably partners from across the globe, from Australia to Japan to South Korea. NATO's partnership with other countries is likely to remain a success story, as demonstrated by the huge International Security Assistance Force coalition as well as the inclusion of Gulf countries in the Libya operation. Indeed, the nature of today's security challenges makes NATO's success increasingly dependent on how well it cooperates with others, whether the issue is peace-keeping, cyberdefense, non-proliferation, counterterrorism, or energy security. Hence, enhancing NATO's "connectivity" (NATO Secretary General Rasmussen) is a precondition for its future as viable security provider. For this reason, the expansion of NATO's partnerships, to eventually even include relations with China and India, is both logical and feasible. Moreover, as other institutions are gradually accepting NATO as a partner in certain contingencies, there is room for further progress.

This progress should eventually also extend to the NATO-EU relationship, which is perhaps the most important of all, yet thus far has remained nervous and incomplete. While certain national sensitivities of NATO Allies and EU members must be respected, the urgency for closer coordination and cooperation between both organizations is greater than ever. Many of the new challenges are both internal and external in nature. For example, terrorism can be home grown or imported, while protecting cyber and energy infrastructures are essentially national responsibilities. This poses entirely new coordination challenges for all actors involved. A stronger NATO-EU relationship would be a major step toward overcoming such challenges.

Another part of a better connected NATO is a sustained relationship with the private sector. Just as the urgency to enhance NATO's cyberdefense

capabilities will lead to closer ties with the software companies, the need to develop a coherent approach to energy security will require NATO to reach out to private energy companies. Creating such new relationships will be challenging, since national business interests and collective security interests may sometimes prove to be irreconcilable. Still, the nature of many emerging security challenges makes the established compartmentalization of responsibilities between the public and private sectors appear increasingly anachronistic.

Third and finally, Allies must use NATO as a forum for a sustained political dialogue about broader security developments. While NATO is engaged on several continents, its “collective mindset” is still largely euro-centric and reactive. As a result many NATO members approach discussions on potential future security issues only hesitantly, worrying that NATO’s image as an operations-driven alliance will create the impression that any such debate was only the precursor to military engagement. While such misperceptions can never be ruled out, the allies should nevertheless resist making themselves hostages to the risk of a few false press reports about NATO’s allegedly sinister military intentions. Indeed, the true risk for NATO lies in the opposite direction: by refusing to look ahead and debate political and military options in meeting emerging challenges, the Allies would condemn themselves to an entirely reactive approach, thus foregoing opportunities for a pro-active policy.

Such a culture of debate is all the more important as many new security challenges do not affect all Allies in quite the same way. A terrorist assault or a cyberattack against just one Ally will not necessarily generate the collective sense of moral outrage and political solidarity that one could witness after “9/11.” Consequently, political solidarity and collective responses may be far more difficult to generate than in the past. Admitting this is not fatalism. It is simply a reminder that the new threats can be divisive rather than unifying if allies do not make a determined effort to address them collectively. On a positive note, there are some indications that this cultural change in NATO has finally begun, as Allies

have become more willing to discuss potentially controversial issues in a brainstorming mode. This welcome development must now be sustained by beefing up NATO’s analytical capabilities, including improved intelligence sharing and longer-range forecasting. Over time, these developments should lead to a shift in NATO’s “culture” toward becoming a more forward-looking organization.

CONCLUSION: APPLYING THE “NOAH RULE”

The paradigm shift away from deterrence and toward prevention and resilience constitutes an enormous challenge both for individual states as well as for alliances. A security policy that accepts that certain threats cannot be prevented through deterrence, and that, thus, some damage will inevitably occur, will be difficult to explain to populations that have become used to near-perfect security. Thus, such a policy will be charged as being fatalistic or scaremongering, while others will interpret it as an alibi by governments to spy on its citizens, or simply as an excuse for increasing defense budgets. And yet the governments of modern industrial societies have no choice but to admit to their citizens that in an era marked by climate change, proliferation, terrorism, and resource scarcity neither the individual state nor an alliance can still offer near-perfect protection. At the same time, governments have to lobby for new forms of protection and consequence management, yet without creating a climate of fear and uncertainty.

All this amounts to a tough sell. However, inaction would ultimately be more expensive. No one has expressed this better than one of the world’s richest individuals, Warren Buffett. The famed U.S. investor had long been thinking about the question of how major disasters would affect the insurance business. But he had not turned his reflections into concrete action. In a letter to his shareholders, written a few weeks after the tragedy of “9/11,” Buffett admitted that he had violated the “Noah rule”: “predicting rain doesn’t count, building arks does.”