Article 5 and the Strategic Concept

Remarks at the NATO Defense College Conference

The Future of NATO's Nuclear Deterrent:
The New Strategic Concept and the 2010 NPT Review Conference

Rome, 2 March 2010

Dr. Maria Mälksoo, ICDS

Throughout the discussions of the new strategic concept of NATO, we have witnessed an almost ritual rhetorical commitment to sustain the collective defense clause as the core mission of the Alliance in the tumultuous contemporary security environment. As an undercurrent to this theme, it is often hastened to add, that the character of potential Article 5 challenges is continuing to evolve. This is precisely the point I would like to elaborate upon in my remarks today. As you would probably expect from someone coming from a new member state of the Alliance, there is, of course, a traditional Article 5 content to be re-emphasized in the light of the new strategic concept. The East European member nations of NATO have been quite vocal in expressing their need of collective reassurance via routinized contingency planning, capability generation and practical military activity in the region in order to buttress their sense of security against possible contenders. Yet, besides the undeniable importance to give significantly more practical substance and visibility to the collective defense commitment in the eastern fringes of the Alliance – both planning- and reinforcement exercises-wise, there is still another burning issue to address in connection to Article 5 and the new strategic concept: namely, the question of how to regard the so-called "new" security challenges, such as cyber and energy contingencies, in the context of Article 5 of the Washington Treaty. Or to put it in layman's terms, could the looming non-traditional security challenges invoke the application of NATO's Article 5 in case their consequences would be of severity equal to the use of physical force?

It could be argued that invoking the collective defense clause after the 9/11 attacks on the United States already constituted a conceptual stretching of the traditional understanding of an armed attack against a member state of the Alliance – to that date generally conceived of as originating from another state actor, not a non-state terrorist grouping, even if an arguably state-sponsored one, as was the case with Afghanistan. The crux of the problem with re-iterating the substantive contents of the core mission of the Alliance – that is, its collective defense clause – in the new strategic concept therefore lies in finding a careful balance between the traditional and contemporary security challenges that could potentially trigger Article 5.

1. The key issue

According to Article 5 of the Washington Treaty, *[T]he Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North*

Atlantic area. The key question is thus: whether (and if indeed, then on what conditions) cyber attacks (or any other attacks on critical infrastructure, including critical information infrastructure of a NATO member state) could be qualified as "armed attacks" in the sense of NATO's Article 5 and thus fall under the rubric of the use of force as defined in the United Nations Charter Article 2 (4)? After all, neither the Washington Treaty nor the UN Charter as its spiritual basis specifies which *arms* are referred to in their respective delineations of an "armed attack".

Legally speaking, there is yet another issue at stake here: from the question quoted above stems the issue whether or not states could use physical force (and not solely political or cyber defense devices) as a self-defense measure (be it individual or collective as outlined in the NATO Treaty and the UN Charter Article 51) in order to retaliate the attempts to undermine their security with non-traditional means if and when these should result in causing real threat or physical damage to their people's lives. In other words, does there have to be physical damage to property or loss of life before a state can exercise the right of self-defense, individually or collectively, as in the framework of NATO's Article 5? As the existing international law on the use of force does not actually prescribe which means could be used by a state for its self-defense – as long as these means are proportional to the extent of the damage caused by an attack on a state and inevitable in order to retaliate the attack, it would follow that a victim of a *de facto* attack could legitimately use military force to retaliate cyber attacks (or any other attacks of the non-traditional kind) that have caused its structures and people real and considerable harm as well. Nonetheless, considering that respective customary law is still developing due to the lack of sufficient state practice and *opinio juris* on the issue, it is rather unlikely that the Alliance would reach a concise politico-juridical "crystallization of the opinion" on cyber and energy security challenges as potential triggers of the Alliance's collective defense provision by the time of the planned completion of the new strategic concept. At the moment, it seems that a much more likely strategy the Allies will opt for is the classification of the above-quoted "new" security challenges under the Washington Treaty Article 4 instead of Article 5. According to this clause, *[T]he Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.*

2. The applicability of Article 5 to the "new" security challenges

In order to analyze the applicability of Article 5 of the Washington Treaty to the so-called "new" security challenges, we should first clarify what makes "new" security challenges qualitatively *new* and thus different from the traditional problems of security. In general, the quality of unprecedented uncertainty and inconclusiveness is taken to be the key characteristic distinguishing "new" threats from the traditional ones. Uncertainty concerns both the identity and goals of potential adversaries, as well as the timeframe within which threats are likely to arise, and the contingencies that might be imposed on the state by others.[1] There is consequently a fundamental uncertainty regarding the capabilities against which one must prepare for as there is a whole gamut of different types of conflict that could potentially occur. Inevitably, this leads to a rather unhappy conclusion that any attempt to somehow objectively

[1] See Myriam Dunn Cavelty (2007) "Is Anything Ever New? – Exploring Specificities of Security and Governance in Information Age", in Myriam Dunn Cavelty, Victor Maner and Sai Felicia Krishna-Hensel (eds) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Aldershot: Ashgate) (19-44), p. 35.

pre-determine the level of risk arising from the "new" security challenges for the Alliance is inherently futile. Clearly, these tensions have also been lurking behind the discussions about the new strategic concept of NATO.

2.1. Cyber threats

Cyber attacks could be regarded as the paradigmatic example of the different nature of contemporary security challenges as compared to the traditional ones: indeed, the issue of *who* has launched an attack, and consequently, who could be held responsible for it, often remains inconclusive and ultimately without definite attribution with many cyber attacks.[2] Accordingly, there is a real possibility to fall into the quagmire of waging a war against a tactical move, or a strategic phenomenon in the vein of the Bush administration's "war against terror" in organizing and activating collective retaliation measures for cyber attacks in case their source has not been conclusively identified. It appears then that it is rather complicated to apply the traditional definition of an armed attack to cyber conflicts, and consequently to invoke NATO's collective defense clause analogously to traditional military attack in case of cyber attacks.

At the same time, NATO has to take into consideration the relative improbability of a traditional armed attack in the Euro-Atlantic space in comparison to the above-mentioned non-traditional security risks. As such a war as is recognized according to the standard definition of the discipline of international relations, that is a military conflict that has resulted in at least 1,000 battle deaths, is relatively unlikely in the Allied territory as compared to the asymmetric threats to the quality of life for the populations of the Allied nations, the need to reconsider the traditional understanding of an "armed attack" from the perspective of NATO's collective defense is nonetheless obvious. What has changed is not just the threat scenery in and of itself, and the perceived significance of the so-called "new" threats by the Allies, but also the understanding of what constitutes a "war" along with the conceptual enlargement of the notion of "life worthy of living". In fact, in order to sustain and protect the "politically relevant life", so to say, or to defend the political sovereignty of a subject, the "battle deaths" in the traditional physical sense are no longer necessarily a *sine qua non* for qualifying an attack as "war". On the other hand, we should also keep in mind that modern conflicts are generally multidimensional. It is thus not necessarily most productive to regard cyber attacks as by definition distinct from a traditional military attack either. Rather, it is quite likely that in contemporary international conflicts, a more traditional kind of disruption would be accompanied by a more or less simultaneous activity on the cyber front as well – as was also the case with the Russian-Georgian war of 2008, for example.

2.2. The problem of identifying the source of cyber attacks

Nonetheless, it remains the case that cyber attacks, just as many other contemporary asymmetric security challenges, rarely allow themselves to be "territorialized". As a rule, they cannot be conclusively connected to a concrete "attacking" state territory or a center of another political power (as was indeed also the case with the cyber attacks against Estonia in 2007). Although theoretically cyber attacks could harm the political sovereignty of a state and

[2] Richard J. Harknett has made the point that it is indeed the problem of attribution, or the inability to conclusively determine the source of the threat, that should serve as the umbrella concept for "new" threats rather than the widely used notion of "asymmetry". – See Richard J. Harknett (2004) "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few", in Emily O. Goldman (ed.) *National Security in the Information Age* (London & Portland, OR: Frank Cass) (13-45), p. 14.

generally hamper its independent functioning, and thus be classified as a potential trigger of NATO's Article 5, a clear definition of a source of an attack would still be necessary for determining the target and focus of the collective response in reality. This can, however, be hardly conclusively determined in case of cyber attacks. Since cyberspace disregards distinctions between national and international, private and public spheres, simply *defining* the expanse of the space to be defended becomes problematic, let alone developing a routine collective coordination system that would be necessary for the successful invoking of Article 5 of the NATO Treaty. Asymmetries indeed abound: defenders must defend everything, all the time, while an attacker can prevail by exploiting a single vulnerability.[3] The qualitative newness of cyber threats thus relies in their separation from the territorial state. It is remarkably difficult to discover the actual origin of cyber attacks, let alone in real time. Cyber attacks could, after all, be conducted in multiple ways, from the hobby hackers and script kiddies to organized crime, political activism and strategic warfare by an adversely-minded foreign power. Traditionally conceived deterrence becomes quite meaningless when the identity of an attacker remains unknown.

Cyber attacks are generally conducted purposefully, but often also entirely unknowingly as a result of computer takeover by individuals and non-state actors which is also why it is so difficult to connect them with a concrete state's willfully adverse activity vis-à-vis another state. State responsibility (and hence also the targeted response by an attacked state(s)) could only be invoked in case:

i) cyber attackers could be qualified as actors supported by state A (or as *de facto* representatives of the state, in case the respective support is conclusively proven);

ii) or, it is successfully proven that state A government was standing right behind the cyber attacks organized against state B.

Harmful activities could range from espionage and the disruption of communication systems (which does not necessarily cause serious damage to people and therefore not exceed the threshold necessary for being qualified as use of force) to cyber attacks causing real and significant harm to people. It is, in fact, only the latter category that crosses the threshold of the use of force, although the other two could also be dealt with in the context of state responsibility.[4] Depending on their particular nature and the juridical nuances of definition, cyber threats could also be qualified as a sub-category of terrorism, which would mean potentially different ways of responding, *inter alia* in the framework of Article 5. Cyber crime is an additional category among cyber security challenges that could be better countered by the European Union (EU) rather than the present means of NATO.

In short, there is no fixed threshold in international law as of yet about the qualification of cyber attacks as the use of force. Consequently, there is also no unequivocal consensus on the issue of the legal justifiability of retaliating cyber attacks with traditional military means in addition to the cyber defense-specific ones. At the same time, the practice of international law is quite pragmatic and most probably there will once be a moment when states declare something in the vein of *"I will know it when I see it"*. It is evident that we are not quite there as of yet, even though the Alliance has, by now, a cyber defense policy and cyber defense

[3] Mark Thompson (2010) "U.S. Cyberwar Strategy: The Pentagon Plans to Attack", *The Time Magazine*, 3 February.

[4] See Erki Kodar (2010) "Computer Network Attacks and the Grey Areas of *Jus ad Bellum* and *Jus in Bello*", *The Baltic Yearbook of International Law* (forthcoming), for further discussion.

concept. It is quite clear that the qualification of cyber attacks in the spirit of the fundamental solidarity clause of Article 5 of the Washington Treaty will be decided *ad hoc* in the actual practice of the Allies, short from concluding a politically binding agreement, let alone an international law treaty on the issue in the near future.

2.3. Can cyber attacks be qualified as an "armed attack"?

A majority of acknowledged international law scholars are of the opinion that cyber network attacks can be regarded as an armed attack only in case their consequences are equal to those of a physical armed attack (for instance, causing an airplane to crash by disabling an air traffic control system, or bringing about the meltdown of a nuclear power plant by hacking into its control system).[5] Incurrence of real and extensive physical damage as a result of a cyber attack is therefore the pre-requisite to regard it as an armed attack, mere economic pressure and political coercion would not quite amount for being qualified as such.[6] Hence, it is inevitable that the consequences of cyber attacks should be evaluated case-by-case to ascertain whether or not they are similar to the consequences of an armed attack. A proactive settlement of a respective general rule is therefore quite problematic.

Cyber attacks against critical digital infrastructures regulating energy and utilities, financial services and transport networks could seriously endanger the smooth functioning of the economy of a state, the sustainability of its critical infrastructures as well as its societal coherence. Cyber attacks could also be targeted at particular defense networks, thus hampering the government's communicative ability in crisis and spreading general panic and a sense of demoralization among the population. In certain extreme cases then, if the above-mentioned stringent criteria is applicable for qualifying cyber attacks as the use of force, adverse cyber activity could indeed invoke Article 5 of the North Atlantic Treaty.

An important issue in determining whether or not cyber attacks should be qualified as Article 5-type of threats lies in their connection to the vulnerability of critical infrastructures more broadly. In other words, if the respective connection would be more-or-less automatic and inclusive then the case for handling cyber attacks under Article 5 analogously to traditional armed attacks would be much stronger and solidly based. Critical infrastructures are usually referred to include water and food provision, health care, transportation, energy, and telecommunications networks, as well as financial services. However, some analysts refute the assumption of automatic vulnerability, regarding linking computer network vulnerability to critical infrastructure vulnerability as misleading, since the latter – especially in large market economies, are arguably more distributed, diverse, redundant, and self-healing than is generally assumed, rendering them thus less vulnerable to attack.[7]

---

[5] See Kodar (2010) for further elaboration.

[6] It has been suggested that if a cyber attack meets the following criteria then it strongly resembles armed force and could come under the purview of the UN Charter Article 2 (4): i) severity (physical injury or destruction); ii) immediacy (high degree of immediacy of consequences); iii) directness (consequences closely linked to the act of force); iv) invasiveness (high level of intrusion on the rights of the targeted state); v) measurability (consequences easily ascertainable); vi) presumptive legitimacy (presumption of impermissibility until proof of self-defense). – Schmitt quoted via Marco Benatar (2009) "The Use of Cyber Force: Need for Legal Justification", *Göttingen Journal of International Law* 1 (3).

[7] This perspective seems to represent strictly the experience of the US, however, and does not necessarily apply to the case of Estonia, for instance. – See further James A. Lewis (2002) *Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats* (Washington: Center for Strategic and International Studies).

In order to assess the actual vulnerability of critical infrastructures to cyber attacks, a detailed evaluation of redundancy for each target infrastructure,[8] along with the normal rates of failure and response, the degree to which critical functions are accessible from public networks, and the level of human control, monitoring, and intervention in critical operations is necessary.[9] There are two main reasons why this is difficult or even impossible: first, there is hardly any public or readily available data concerning the vulnerability of critical systems. Layers of classification cover the respective information, nor are private companies particularly willing to volunteer such information. In addition to the problematic accessibility of the relevant information, the assessment of the actual vulnerability of critical infrastructures is further complicated by the fact that "criticality" cannot be established on the basis of this data alone. On the one hand, what is considered critical is always in flux, constantly changing; on the other, the criticality of an infrastructure or service can never be identified preventively, but only *ex post facto*, after a crisis has already occurred and the respective conclusions drawn from an evaluation process. Last but not least, it is important to keep in mind that any potential vulnerability, in order to become realized as a threat, needs the availability of actors with the capability and motivation to attack this vulnerability.[10]

Following NATO's cautious rhetoric and policy line so far, it seems most probable that cyber security challenges would be tackled rather in the framework of Article 4 of the North Atlantic Treaty in which case Allies will enter into consultations if the territorial integrity, political independence or security of any of the members should be threatened. It would appear as particularly important to understand a *threat to security* broadly and to keep the threshold for calling upon allied consultations as low as possible, so that Article 4 would indeed be accessible and available in case of need.

At the moment, there is no political consensus, let alone an international legal one, on the issue whether or not cyber threats could be qualified as use of force according to the UN Charter Article 2 (4) that would activate the self-defense provisions of the North Atlantic Treaty framework. According to Article 2 (4) of the UN Charter, *all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*. Consequently, it is also difficult to determine unequivocally the specifics of individual and collective self-defense, the right of which is provided in Article 51 of UN Charter, in case of cyber attacks. It should be kept in mind, however, that even if cyber force cannot be *a priori* defined as use of force as traditionally understood in international law, it constitutes nonetheless a violation of the principle of non-intervention in matters within the domestic jurisdiction of another state. Either way, a cyber attack could constitute a violation

[8] Estonian Cyber Security Strategy underscores the distinction between *critical infrastructure* and *critical information infrastructure*. The former refers to those assets, services and systems (or their parts and the connections between them) which destruction, damaging or overtaking could endanger people's lives or well-being or bring about the demolition of the assets, services, systems or their parts, or extensive economic damages, and diminish the credibility of a state, undermine its image and hamper its general functioning. *Critical information infrastructure* refers, in turn, to those components of information infrastructure that are themselves critical or utterly necessary for the functioning of a critical infrastructure. – See *Cyber Security Strategy 2008-2013* (2008) (Tallinn: Ministry of Defense).

[9] Cf. Lewis, 2002, 10.

[10] See Cavelty, 2007, 34.

against the principle of state responsibility, as it is fixed in the International Law Commission Articles on State Responsibility (2001) and approved by the UN General Assembly.[11]

Whether or not concrete cyber attacks should trigger the collective defense provision of NATO Article 5 will remain to be decided *ad hoc* by the Allies in the conceivable future. Clearly, the implementation of Article 5 in case of cyber network attacks will be closely related to the implementation of Article 4 of the North Atlantic Treaty. Once a cyber conflict actually crosses the threshold of armed attack, the legal and policy mechanisms created in peacetime and used to foster Article 4 cooperation, most importantly the exchange of the information concerning the threats and possible defensive measures, will be the key basis for coordinated response.[12]

While cyber security will undoubtedly be high upon NATO's agenda in the near future to come, the main emphasis of NATO's activities will most probably be on the prevention of threats, "preventive defense" as well as building up Alliance's redundancy against possible attacks. Estonia's cyber security strategy defines decreasing the vulnerability of the cyber space, prevention of cyber attacks and restoration of the activity of information systems as quickly as possible in case of an attack as the main tasks in securing the national cyber space (if such a thing can even be reasonably distinguished, of course). NATO's cyber defense concept should follow the same core guidelines.[13] The main strategic goal of the Alliance should be deterrence through denial, through improving one's own defensive capabilities against potential cyber attacks as well as developing an adequate capability to undermine opponent's offensive capabilities through a pre-battle information suppression operation, designed with an aim to dissuade the opponent from attacking in the first place.[14] Traditionally conceived deterrence is difficult to apply to the so-called "new" threats since deterrence assumes the scope of an attack can be quickly determined, the source of attack clearly recognized, and the likely damage from offensive attack assessed along with the recognition of the possible gains motivating the opponent.[15] The assumption of traditional deterrence about an identifiable opponent may not necessarily be possible in the context of the security trends of the information age, especially considering that asymmetric attacks are often launched by non-state actors.

2.4. Article 5 and energy security

Taking into consideration the multidimensionality of the notion of energy security, the difficulties in trying to make NATO responsible for securing the economic aspects of energy security and guaranteeing the sustainability of energy networks are immediately evident. Regarding its current profile, NATO is not the most suitable organization for organizing its members' energy procurement security or their "energetic independence" (or non-reliance on import, at least not solely), let alone guaranteeing the stability and multiplicity of energy

[11] For example, the DDoS (*Distributed Denial of Service*) attacks against Estonia in the spring of 2007 were intended to create social unrest in response to the domestic policies of a democratically elected government, thus constituting an intervention vis-à-vis a democratic system.

[12] See Toomas Hendrik Ilves (2009) *President Ilves at the Conference on the Lgeal and Policy Aspects of International Cyber Conflict*, Tallinn, 9 September; available at http://www.president.ee/en/speeches/speeches.php?gid=130309 (last accessed 4 February 2010).

[13] Cf. Estonian Cyber Security Strategy, 2008, 7.

[14] Cf. Matt Bishop and Emily O. Goldman (2004) "The Strategy and Tactics of Information Warfare", in Emily O. Goldman (ed.) *National Security in the Information Age* (London & Portland, OR: Frank Cass) (113-39), p. 134.

[15] See Harknett, 2004, 34.

providers and the diversity of energy sources. NATO should rather embrace critical infrastructure security broadly conceived, looking after its sustainability and organizing its defense, if necessary, including being prepared for major accidents, terrorist attacks, acts of sabotage and incidents of organized crime affecting large critical infrastructures of the Allies. A more ambitious idea of organizing defense on a permanent basis in order to secure major Allied energy structures from the oil and gas fields to the protection of pipelines and energy transit routes on the high seas is nonetheless still an issue of great contention among the Allies. Whether or not the use of the "energy weapon" by willful disruption or suspension of energy flows and thus extensive harm caused for people's lives and the functioning of the major critical infrastructures of a state should belong under the purview of Article 5 of the Washington Treaty, as has been suggested by an influential US Senator Richard Lugar,[16] for instance, has similarly remained a subject of heated debate within the Alliance.

After all, the retaliation of a physical attack against energy infrastructures requires different policies and capabilities than reacting to the disruption of energy supplies without applying physical coercion or violence (such as the radical decrease or cutoff of energy, rises of energy prices, embargoes etc.). All the same, the suspension of gas supplies in some European ally in the middle of winter could yield to significant casualties as well as economic damages with consequences equal to those of an armed attack. According to the position introduced by Senator Lugar, the "energy security Article 5" would not necessarily require a NATO military response in order to counter attempts to manipulate energy for international political gain, but rather a collective solidarity cause to re-supply the member state(s) affected by an aggressive energy suspension via alternative mechanisms and sources. According to Lugar's vision, NATO should identify alternatives to existing pipelines or develop alternative energy sources, in order to re-supply its members in case of need. It should also advance strategies and mechanisms to re-supply victim of an energy blackmail or cutoff in case of an emergency as well as guarantee the necessary infrastructures to be present in case of a possible attack. The logic behind such a route of action is quite simple indeed: a clearly coordinated and as unambiguously outwardly communicated reaction of the Alliance to the possible blackmail with an "energy weapon" would in and of itself constitute a deterrent of a kind.

Nevertheless, there is no consensus in the Alliance about whether or not NATO's field of responsibility could also be enlarged to include the management of emergency energy reserves. The distinct energy security vulnerabilities of the European allies and the US, let alone the different levels of "energetic vulnerability" among the European allies, have not alleviated the finding of an Allied consensus on the issue. Some European allies, such as France, would clearly prefer to give the "energy security Article 5" as envisioned by Senator Lugar to the jurisdiction of the European Union instead. Yet, it is precisely the inability of the EU to create an adequate common energy policy that has brought about the increasing discontent of voices like Lugar's over the handling of energy security problems in Europe to this date.

NATO declares itself to focus mostly on the issues of guaranteeing critical infrastructure security, lending support to member states in order to protect their respective energy infrastructures if asked, following general trends, assessing risks and offering crisis management. It is nonetheless evident that developing a common management system for energy crises still needs considerable work to be done in the Alliance. NATO should continue its activities in developing necessary mechanisms and models of action in crisis situations for

[16] See Richard Lugar's remarks at the NATO summit in Riga, March 2007.

mutual support. Equally important would be to specify and strengthen the modes of action in case of major accidents and emergencies or energy supply crises. Again, the weight of emphasis of NATO's critical infrastructure protection lies on prevention, in order to minimize preemptively the probability of energy cut-offs or attacks against respective infrastructures, as well as their possible consequences.

In the conceivable future then, energy security problems will also rather fall into the competence of Article 4 of the North Atlantic Treaty. In the final analysis, the EU would be a more competent and suitable organization to address the different dimensions of energy security than today's NATO due to its multiple economic and political means. The preventive action vis-à-vis energy-related security risks should therefore mostly be undertaken in the framework of the EU's common energy policy, which is, however, still suffering from significant birth pains. Energy-related crisis management by NATO would already demonstrate the failure of political solutions. Yet, it is still evident that the successful handling of energy security challenges can only come about in the mutually supportive cooperation of the EU and NATO. Hence the need to specify more thoroughly NATO's activities in preventing energy security challenges and managing energy crises in the new strategic concept as well.

3. Conclusion

At the moment, it cannot be conclusively answered whether the challenges relating to cyber and energy security could be unequivocally qualified as falling under the purview of Article 5 of the North Atlantic Treaty. There is no way but to speculate as we are currently ourselves living in the midst of the processes specific to the information age, having thus to react to cyber and energy security problems while they occur, witnessing them and trying to deal with them in real time. We should, however, clearly distinguish between the two levels of the question here: namely, what is the existing normative state of the art at the moment (or existent law, *lex lata*) and what would be the law we would like to have on the issue in the future (*lex ferenda*)?

If we ask, for instance, whether the existing law and the state of the art (i.e. state practice) would enable to construe cyber attacks under Article 5, the answer would rather be on the negative. That is not because the existing law would exclude the possibility, but rather for the reason that Article 5 does not purposefully address this issue. The sole exception would be provided by the extraordinary cases quoted above (that have not yet been fully observed as such in the Allied practice to date). Regarding *lex ferenda*, however, we have to take into consideration that NATO can give new extended substance to its legal duties only as a result of extensive consultations and consensus-building. It has to also be acknowledged that the future interpretation of the Washington Treaty would need to be "in sync" with the mainstream interpretation of the UN Charter. The latter is, however, due to its membership specifics (i.e. its majority being constituted of small non-Western states) rather conservative in regard to the use of force. There is a general fear that strong states would seek excuses for using force against weak ones.[17]

[17] The International Court of Justice rule of 1986 on the case of *The Republic of Nicaragua v. The United States of America* was symptomatic in that context, as the main issue concerned the right to legitimately resort to armed self-defense by invoking Article 51 of the UN Charter. The Court's rule maintained that not even all violations of Article 2 (4) (that is, use of force, such as supporting guerillas across the border) do not automatically qualify as an "armed attack" in the meaning of Article 51. This position has, of course, been severely criticized as well,

Regarding the specifics of cyber and energy security challenges, it is clear that these could not be regulated by state means only – close cooperation with the private sector is inevitable. Since cyberspace disregards distinctions between national and international, private and public sphere, already the definition of the expanse of what is to be defended becomes incredibly complex, let alone developing the coordination that would be necessary for security. An additional difficulty with multidimensional conflict, for instance in case traditional and cyber force are used simultaneously, is that the signaling necessary for deterrence regarding a state's will and capability to retaliate a potential attack is open to greater misinterpretation – either because the threat is made too imprecisely or because it is directed too narrowly.[18] The challenge to calibrate deterrence so that it would constrain options of both state and non-state actors, traditional and non-traditional threats, as well as weave nuclear and conventional aspects in a sensible way becomes all the more daunting, yet important, against that backdrop.

At the end of the day it might be even worthwhile to keep the constructive ambiguity about the threats potentially triggering the backbone of the North Atlantic Treaty – its collective defense commitment as provided in Article 5. A too detailed and specific a count of Article 5 threat spectrum might lead to a situation where some challenge that is perceived by a member state as existential has nonetheless remained out of the enumeration of threats potentially invoking Article 5. The possibility of providing an aggressor with extra means by too detailed a provision of threats in international law was, in fact, a danger already recognized in the pre-World War II discussions of international law. The drafters of the new strategic concept of the Alliance would be indeed wise not to forget this old truism.

especially in the United States. Nonetheless, it could still be regarded as an evocative indicator of the general reluctance of international community to interpret the existing law in a flexible manner.

[18] See Harknett, 2004, 33-35.