CYBER SECURITY AND DEFENCE FROM THE PERSPECTIVE OF ARTICLES 4 AND 5 OF THE NATO[250] TREATY

Ulf Häußler[251]

INTRODUCTION

In the recently published report 'NATO 2020: Assured Security; Dynamic Engagement' which contains the analysis and recommendations of the group of experts on a new strategic concept for NATO[252], the experts observed that:

> "… the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5."[253]

This observation points at the key challenges cyber activities pose from a legal perspective on international peace and security. It can easily be rephrased as a question: In what circumstances and under what conditions would NATO's collective security and defence mechanisms be triggered by cyber activities? The present paper will explore some initial answers to this question. For this purpose, it will revisit and explain the language of the North Atlantic Treaty in lights of relevant NATO practice, identify possible cyber threats and assess them against the thresholds contained in Articles 4 and 5 of the North Atlantic Treaty, and discuss key challenges which may arise in the course of developing NATO responses (noting that such challenges may also affect the effort to include the notion of effective deterrence[254] in the Alliance's approach to cyber defence). While based on legal analysis of the North Atlantic Treaty and relevant international law, this paper

250 The original title of the article "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the North Atlantic Treaty" was shortened by the editor for technical reasons.

251 Assistant Legal Advisor (Operational Law), Allied Command Transformation (NATO ACT, Norfolk/Va., USA). The views expressed herein are my own; they do not necessarily correspond with the official position of NATO or the Headquarters, Supreme Allied Commander Transformation. The author expresses his gratitude to Ms Simona Rocchi, Legal Advisor to NC3A, Mr Jude Klena, Counsel within the U.S. Navy, and Ms Katharina Ziolkowski, Legal Advisor within the German Armed Forces, for insightful comments and critique of an earlier version of this paper.

252 The experts report is available at http://www.nato.int/strategic-concept/expertsreport.pdf (last visited 16 June 2010).

253 Cf. the experts report at 45.

254 Cf. the experts report at 11 and 20.

focuses on the legal policy questions associated with the effort to fully integrate cyber defence in NATO's toolbox.

PRELIMINARY REMARKS

In coaching their above observation in the subjunctive mood, the experts have indicated that their analysis does not amount to a statement of NATO policy concerning the interpretation and application of Articles 4 and 5 of the North Atlantic Treaty. This being so, the observation indicates that to date no policy consensus of that nature exists in NATO[255]. In the absence of policy decisions and policy consensus, one important, probably the key contribution to the interpretation and application of international treaty law – aptly identified as represented by 'any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation' by Article 31(3)(b) of the Vienna Convention on the Law of Treaties – is missing.

In the context of international peace and security, the significance of policy decisions and policy consensus for the interpretation and application of international law oftentimes by and large overlaps with their nature as acts embodying the primacy of policy over the use of military force. While contemporary decisions to use a nation's and/or an alliance's capabilities in pursuance of collective defence may involve the interpretation and application of international law and as such also be expressions of legal policy, they equally reflect the insight, long ago shared by Carl v. Clausewitz, " ... that war is not merely an act of policy but *a true political instrument*, a continuation of political intercourse, carried on with other means".[256]

Considering the highly political nature of such decisions, the associated interpretation and application of Articles 4 and 5 of the North Atlantic Treaty may come with no less ambiguity than any equivalent effort made with respect to many another relevant law-making international treaty. To give but two examples for the prevailing level of ambiguity: neither has any "declared war"[257] occurred since 1949

255 Several scholars stress the importance of consensus regarding the interpretation and application of the rules concerning the jus ad bellum to the use of cyber capabilities. See e.g. Matthew Holsington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, in: 32 B.C. Int'l & Comp. L. Rev 439 (2009) at 439 and 454; William Yurczik & David Doss, Internet Attacks: A Policy Framework for Rules of Engagement (online at arxiv.org/pdf/cs/0109078; last visited 31 August 2010), at 17; cf. also Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, in: 106 Michigan Law Review 1427 (2008) at 1430 (noting the lack of consensus regarding the application of the *jus in bello* to cyber warfare).

256 Carl v. Clausewitz, On War, translated by Michael Howard and Peter Paret and published by Alfred A. Knopf in the Everyman's Library series, New York - London - Toronto 1993, Book One Chapter One Part 24 entitled "War is Merely the Continuation of Policy by Other Means" (my emphasis).

257 This language is borrowed from Article 2 of GCs I-IV.

(despite the considerable number of international armed conflicts in that time-frame) – if only because it may have been easier for States to obtain authorisation by the UN Security Council under Chapter VII or rely on their inherent right of self-defence (doing which also counters allegations that they might have breached Article 2(4) of the UN Charter) – nor has the UN Security Council made any significant use of the options available to it for the purpose of characterising a situation under Chapter VII of the UN Charter ("existence of any threat to the peace, breach of the peace, or act of aggression"[258]), options which it has by and large replaced by the phrase "threat to international peace and security"[259]. What is good for the UN Security Council would seem to be equally good for the North Atlantic Council: interpretation and application of pertinent legal bases will more likely be guided by practical policy concerns than by a desire to win an award for perfectionism in matters of legal doctrine. It follows that a search for circumstances and conditions in which cyber activities would trigger NATO's collective security and defence mechanisms will not necessarily yield an abundance of clear-cut criteria early on; rather the degree of clarity will grow as the related policy consensus matures.

ARTICLES 4 AND 5 OF THE NORTH ATLANTIC TREATY

The North Atlantic Treaty has established NATO as a collective security and defence alliance involving cooperation in matters of security and defence policies as well as military operations. Initially focused on defence of its nations' territories, NATO's role as a security provider has been transformed in recent years; it now includes the organisation's preparedness – where possible in a lawful and legitimate manner – to tackle, prevent, or pre-empt threats at their source[260].

NATO's collective security and defence mechanisms are primarily entrenched in Articles 4 and 5 of the North Atlantic Treaty[261]. Article 4 provides that:

> '[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'.

Article 5 specifies that:

> '[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

258 See Article 39 of the UN Charter.
259 The UN Security Council has used this language in multiple resolutions adopted in application of Chapter VII of the UN Charter.
260 Strategic Concepts 1993 and 1999.
261 For the full text of the North Atlantic Treaty see http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

> agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked …'.

These provisions indicate that it is the Nations' prerogative to determine whether they consider themselves exposed to a threat or under armed attack. However, they do not create any automaticism whatsoever concerning the response in such cases[262].

Whilst they are NATO's key legal bases, Articles 4 and 5 are not the sole legal bases for NATO action. As confirmed by consolidated practice, they are supplemented by Article 7 of the North Atlantic Treaty – which keeps the door open for NATO and NATO-led operations in support of the purposes of the United Nations – and appropriate implied powers of the organisation.

The emergence and growth of NATO's security policy *acquis* through policy decisions concerning strategy – embodied *inter alia* in the Strategic Concepts 1993 and 1999 as well as the Comprehensive Political Guidance 2006 – as well as operations – all NATO and NATO-led operations require approval by the North Atlantic Council – demonstrates the flexibility of the ensemble of these legal bases for decision-making on Alliance action[263]. NATO Nations' related decisions confirm that they wholeheartedly approve the flexible interpretation and application of the North Atlantic Treaty. The most important decisions of this nature are embodied in the integration of new members in the organisation by virtue of various Protocols to the North Atlantic Treaty to which all NATO Nations have become Parties. Although the Alliance's security policy *acquis* is not expressly mentioned in these Protocols, the process leading to their approval and adoption – the Membership Action

262 As stressed by Beckett, each NATO Nation is 'the judge of whether armed force is required or whether other action will suffice' (The North Atlantic Treaty, the Brussels Treaty, and the Charter of the United Nations, London: Stevens & Son, 1950, at 28) regarding the application of Article 5. See also Lawrence S. Kaplan, NATO 1948: The Birth of the Transatlantic Alliance (Rowman & Littlefield Publishers, Canham/MD 2007), at 204; and, by the same author, NATO Enlargement: The Article 5 Angle, in: The Atlantic Council of The United States, Bulletin Vol. XII, No. 2, February 2001, at 2-3. The entire Bulletin addresses the policy dynamics associated with the 'less than clear commitment by the United States' which nevertheless 'is still the symbol of U.S. commitment to its European partners' (at 3/4, respectively). The post-9/11 practice of NATO and its Nations has confirmed this position.

263 A detailed analysis of NATO's security policy *acquis* would exceed the objective and scope of this paper. Suffice it to say that this *acquis* entails not only the facilitation of coalition-style multinational support of collective self-defence (Operation Enduring Freedom) but also NATO/NATO-led operations which the North Atlantic Council may approve in support of collective self-defence (Operation Active Endeavour); a UN Security Council Resolution (e.g. IFOR/SFOR/NHQ Sarajevo; KFOR, ISAF; NTM-I; NTM-A; Operation Ocean Shield and its predecessors) or the principles of the United Nations (e.g. Operation Allied Force); a request made by a sovereign state (e.g. Operations Amber Fox/Fox/Allied Harmony; Pakistan Earthquake Relief) or an international organisation (e.g. the African Union). Such operations may cover the entire spectrum of education, training and exercises support; humanitarian relief; counter-insurgency; and other forms of low as well as high intensity conflict, in particular in the framework of Non-Article 5 Crisis Response Operations.

Plan which prepares potential new members to join NATO in accordance with a decision taken by all NATO Nations – requires implementation of NATO's security policy *acquis* by candidate countries[264]. NATO Nations' ratifications of the relevant Protocols should hence be considered as acts confirming the security policy *acquis* in its capacity as a necessary condition for joining NATO. Moreover, NATO Nations have on numerous occasions reinforced the Alliance's security policy *acquis* through their decisions to approve, and contribute forces to, NATO/NATO-led operations. In the absence of indications to the contrary, the policy decisions referred to should be regarded as suggesting the existence of subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions as envisaged by Article 31(3)(a) of the Vienna Convention on the Law of Treaties, and the associated conduct of NATO and its Nations should be regarded as supplementing practice of the nature contemplated by Article 31(3)(b) of the Vienna Convention on the Law of Treaties[265].

This paper argues that the North Atlantic Treaty's flexibility also empowers NATO – from both a policy and a legal perspective – to include the full spectrum of cyber security and defence policy as well as operations in its toolbox.

THREATS & THRESHOLDS

To date, few instances of practice in the application of the thresholds for NATO involvement and action, respectively, specified in Articles 4 and 5 of the North Atlantic Treaty, have been reported. As regards Article 5, NATO's response to the September 11 attack on the United States of America is the only known example. Article 4 has been formally used in one reported case; in February 2003, Turkey asked for consultations concerning its defence needs arising in light of the impending resumption of hostilities against Iraq[266]. The absence of further identifiable practice may be due to the fact that in engaging the North Atlantic Council regarding threats to their security NATO Nations seem not to have expressly invoked this provision: if only to keep the consultations they initiated focused on substance rather than the

264 Under the heading of 'Defence and military', the Membership Action Plan focuses on the ability of the country to contribute to collective defence and to the Alliance's new missions. This ability is contingent on the implementation of the Alliance's security policy *acquis*. See the online version of the NATO Handbook at http://www.nato.int/docu/handbook/2001/hb030103.htm (last visited 02 august 2010).

265 It would seem that Article 31(3) of the Vienna Convention on the Law of Treaties would not establish a very high threshold for the purposes of establishing that decisions or action represent subsequent agreement or practice, respectively, as indicated by the use of the word 'any' as qualifier in this respect.

266 See Paul Gallis, NATO's Decision-Making Procedure (CRS Report for Congress, Order Code RS21510, 05 May 2003; online at http://www.fas.org/man/crs/RS21510.pdf (last visited 29 August 2010)), at 1.

question of whether the Article 4 threshold was actually crossed. For instance, in discussions the fact that the North Atlantic Council discussed the 2007 cyber attack faced by Estonia has repeatedly been cited as an example of Article 4 consultations despite the fact that neither Estonia nor the Council as a whole mentioned this provision. As a result, there is rather limited NATO practice to rely on as the primary source of interpretation concerning Articles 4 and 5 of the North Atlantic Treaty.

NATO AND UN LEGAL BASES COMPARED

In the near complete absence of practice, it is apt to explore further sources of interpretation. Apart from utilising scholarly writing which sheds light on the drafting history of the North Atlantic Treaty, comparative analysis of the development of related UN Charter provisions might be a source of inspiration for the interpretation of these provisions.

Articles 4 and 5 of the North Atlantic Treaty have a significant terminological overlap with Articles 2(4) and 51 of the UN Charter, respectively. Since such terminological overlap indicates that there may be a conceptual overlap, as well, the interpretation and application and are to a large extent capable of developing in unison. Whether, and to what extent, they have indeed developed along the same lines is revealed by policy decisions interpreting and applying them to individual situations. The UN and NATO responses to the attack on the United States on 11 September 2001 provide an ample example of a partly unison, partly different development of both treaties. As will be demonstrated shortly, both the UN Security Council and the North Atlantic Council have taken decisions bringing these attacks within the ambit of the notion of armed attack under Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty. However, neither of these decisions contains an express determination of why the threshold of armed attack was crossed. Accordingly, it is a matter of analysis whether they can be considered to address such legal questions arising with regard to responsibility and attribution as are associated with the fact that the attack was carried out by operatives of a non-governmental party (Al Qaeda), an organisation enjoying material support of the *de facto* government of Afghanistan at the time (the Taliban). Similar questions may arise with respect to cyber security and defence in light of the both empirical and practical relevance of the conduct of non-governmental actors in this field.

DRAFTING HISTORY

The drafting history of the North Atlantic Treaty reveals that threshold questions may not have been the predominant concern in developing the language of

Articles 4 and 5. The most important sources appear to be W. Eric Beckett's analysis concerning the question of whether NATO is a 'regional organization' as defined in Chapter VIII of the UN Charter (a question which he answers in the negative)[267], and Lawrence S. Kaplan's analysis of the level of commitment digestible in the U.S. Senate at the time of the negotiations[268].

Beckett, at the time a legal advisor to the Ministry of Foreign Affairs of the United Kingdom of Great Britain and Northern Ireland, observes that Article 4 has much in common with certain provisions of other collective security agreements[269]; he does not, however, address possible overlaps of Article 4 (or any of the other provisions discussed) and provisions on the UN Charter. At the same time, Beckett explores what relationship may exist between the consultation mechanism established by Article 4 and the right to engage the United Nations in case of looming security threats under Article 35 of the UN Charter[270]. The latter, in his view, does not 'in any way preclude any group of States from consulting on a potential threat to anyone of them' such as e.g. in accordance with Article 4 of the North Atlantic Treaty. According to Beckett: '[s]uch a consultation may have, amongst other things, a bearing on the question whether or not the threat should be brought before the Security Council', and '[n]o doubt if the consultation leads to the conclusion that the threat is sufficiently serious, one or other or all of the parties will exercise the right which they have under the Charter to bring the matter before the Security Council'.[271]

The analysis of Article 5, which 'is the collective self-defence obligation in case of armed attack'[272], likewise reveals similarities. Beckett rightly observes that 'Article 5 of the Treaty uses the same words "armed attack" as occur in Article 51 of the Charter and expressly purports to be based on that Article'[273]. This is confirmed by

267 See in particular Beckett, at 34.
268 Lawrence S. Kaplan, NATO Enlargement: The Article 5 Angle, in: The Atlantic Council of The United States, Bulletin Vol. XII, No. 2, February 2001, *passim*. See also, by the same author, NATO 1948: The Birth of the Transatlantic Alliance (Rowman & Littlefield Publishers, Canham/MD 2007).
269 According to Beckett, Article 4 'is rather similar to the second paragraph of Article 7 of the Brussels Treaty and has certain analogies with Article 6 of the Rio Treaty' (at 26sq). As regards Article 6 of the Rio Treaty (Inter-American Treaty of Reciprocal Assistance, signed at Rio de Janeiro, 02 September 1947; reproduced in Beckett, ibidem, at 51sqq), the difference in wording between Article 4 of the North Atlantic Treaty and Article 6 of the Rio Treaty is not tantamount to any real differences of substance and meaning (*ibidem*, at 21). At any event, as far as possible to establish there is no officially published practice under Article 6 of the Rio Treaty which could be relied on in support of the interpretation of Article 4 of the North Atlantic Treaty.
270 Article 35 of the UN Charter provides that UN member states may bring any dispute, or any situation which might lead to international friction or give rise to a dispute, to the attention of the Security Council or of the General Assembly.
271 Beckett, at 27.
272 Beckett, *ibidem*.
273 Beckett, at 29. See – in a different context (collective self-defence in support of NATO Nations which at the time were not members of the United Nations Organization) – *ibidem* at 31.

Kaplan's observation that the U.S. Senate was determined to ensure that Article 5 would be fully compatible with Article 51 of the UN Charter[274]. Successfully so, as demonstrated by Beckett's analysis of the statement in Article 5 that 'an armed attack against one or more of the Parties shall be considered to be an attack against them all': this language expresses 'precisely what the *inherent* right of *collective* self-defence means'[275].

When they embarked on turning the right of collective self-defence into the foundation of a collective self-defence obligation, NATO Nations have invited questions regarding the nature of this obligation. Kaplan, who compares Article 5 to the collective defence provisions of the Rio Pact and the Brussels Treaty, explains why it was easier for the U.S. to accept a moral rather than a legal obligation, viz. in light of the delicate balance between the constitutional powers of the U.S. Congress concerning declarations of war and the mechanism for setting collective self-defence in motion[276]. By contrast, Beckett's analysis, according to which the obligation under Article 5 is 'several and not merely joint'[277], indicates by using these legal categories that he considers collective defence within NATO to be a legal obligation. Whilst the true nature of the obligation under Article 5 of the North Atlantic Treaty was never determined, it may not have much practical bearing in the first place. NATO Nations have always considered it to be their sovereign decision what support they would provide in an actual case of collective self-defence, and in the one and only practical case, they have not hesitated to provide support in an apparently satisfactory manner.

As indicated earlier, Beckett's and Kaplan's observations and analysis focus on questions not involving the actual meaning of the substantive thresholds contained in Articles 4 and 5 of the North Atlantic Treaty. As regards Article 4, Beckett focuses on the consultation process envisaged by this provision rather than the threshold which may justify that a NATO Nation engages this process by way of requesting consultation. Beckett's analysis of Article 5 confirms that this provision establishes the same threshold as, and has further similarities with, Article 51 of the UN Charter; however, his observations concerning the notion of 'armed attack' in a footnote which merely repeats the essence of the discussion in the U.S. Senate's Foreign

274 Lawrence S. Kaplan, NATO 1948: The Birth of the Transatlantic Alliance (Rowman & Littlefield Publishers, Canham/MD 2007), at 217.
275 Beckett, *ibidem* (emphasis in the original). Moreover, as confirmed by Beckett, the similarity between Article 5 of the North Atlantic Treaty and Article 51 of the UN Charter also extends to the reporting requirement concerning measures taken in collective self-defence and the provision that such measures shall be terminated when the Security Council takes enforcement action (*ibidem*).
276 Lawrence S. Kaplan, NATO Enlargement: The Article 5 Angle, in: The Atlantic Council of The United States, Bulletin Vol. XII, No. 2, February 2001, at 3.
277 Beckett, at 28.

Relations Committee[278] indicate that this threshold did not pose major interpretive challenges at the time of drafting.

COLLECTIVE SELF-DEFENCE IN NATO PRACTICE

The attack on the United States of America on 11 September 2001 (hereinafter referred to as '9/11') represents the only case in which NATO's collective self-defence mechanism was used. The response to 9/11 demonstrates how the UN Security Council and the North Atlantic Council as well as multiple Nations have interpreted the notion of 'armed attack', key to the application of Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty, respectively, in the same adaptive way so as to capture the genuine characteristic elements of the attack.

Following the 9/11 attack, the UN Security Council adopted UNSCR 1368 (2001) dated 12 September 2001 in which it recognised 'the inherent right of individual or collective self-defence in accordance with the Charter' and determined that it '*regards* such acts, like any act of international terrorism, as a threat to international peace and security'[279]. This resolution differentiates between the Chapter VII and self-defence thresholds; while it determined the former to have been crossed[280], it did not make an express determination concerning the latter. On the same day as the UN Security Council, the North Atlantic Council 'agreed that if it is determined that this attack was directed from abroad against the United States, it shall be regarded as an action covered by Article 5 of the Washington Treaty'[281], which it indeed determined, following a briefing on the results of investigations into the attack, on 02 October 2001[282]. Subsequently, the North Atlantic Council authorised Operation Active Endeavour, a maritime interdiction operation in the Mediterranean. NATO also informed the UN Security Council of its invocation of Article 5 of the North Atlantic Treaty[283]. The North Atlantic Council's decision also provides the umbrella for NATO Nations' support to Operation Enduring Freedom,

278 Beckett, at 28 (footnote 12).
279 See para 1 (emphasis in the original) and the last preambular paragraph of UNSCR 1368 (2001), respectively.
280 The UN Security Council has subsequently confirmed this determination. See UNSCR 1373 (2001).
281 See NATO Press Release (2001)124 dated 12 September 2001, online at http://www.nato.int/docu/pr/2001/p01-124e.htm (last visited 07 July 2010).
282 See NATO Topic: Collective Defence, online at http://www.nato.int/cps/en/SID-85648058-8934EDC9/natolive/topics_59378.htm (last visited 07 July 2010).
283 In the Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005), Canada has made reference to 'the notification by the Secretary-General of the North Atlantic Treaty Organization (NATO) to the Secretary-General of the United Nations on the invocation by NATO of article 5 of the North Atlantic Treaty' (*ibidem*). The notification was not circulated in the UN Security Council and, according to information generously provided by the UN Regional Information Centre Brussels to the author, is not accessible in the UN Archives Database, either.

the United States self-defence effort against the *de facto* government of Afghanistan (the Taliban) – the State responsible for the attack – and Al Qaeda – the terrorist organisation whose operatives had perpetrated the attack[284]. Canada's Article 51 report to the UN Security Council is particularly point-on since it expressly links the use of Article 51 to the North Atlantic Council's decision concerning Article 5[285]. Multiple Nations reported to the Security Council that they had taken measures in accordance with Article 51 of the UN Charter[286]; As a result, NATO's collective defence mechanism covers both NATO/NATO-led operations in support of a NATO Nation's self-defence[287] and a NATO umbrella for NATO Nations' support of another NATO Nation's self-defence.

284 The information concerning the responsibility of the Taliban and Al Qaeda available at the time to both the North Atlantic Council and the UN Security Council is reproduced in the Annex to the Letter dated 8 October from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (UN document S/2001/949). On attribution to the State of Afghanistan through its *de facto* government see my paper Der Schutz der Rechtsidee, in: Zeitschrift für Rechtspolitik (ZRP) 2001, 537-541.

285 See the Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005).

286 Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council (UN document S/2001/946); Letter dated 7 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (UN document S/2001/947); Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005); Letter dated 23 November 2001 from the Permanent Representative of France to the United Nations addressed to the President of the Security Council (UN document S/2001/1103); Letter dated 23 November 2001 from the Permanent Representative of Australia to the United Nations addressed to the President of the Security Council (UN document S/2001/1103); Letter dated 29 November 2001 from the Permanent Representative of Germany to the United Nations addressed to the President of the Security Council (UN document S/2001/1103). See also the Letter dated 17 October 2001 from the Permanent Representative of Slovenia to the United Nations addressed to the President of the Security Council (UN document S/2001/987).
Whilst it would exceed the scope and purpose of this paper to provide a full analysis of the legal nature of Operation Enduring Freedom as well the non-U.S. contributions thereto, it may suffice to note that many Nations which later adopted the position that the armed conflict between the U.S. and Afghanistan had come to an end when the *de facto* government was replaced by the Interim Authority established by the Bonn Agreement dated 05 December 2001 continued to contribute forces to Operation Enduring Freedom in the Afghan theater where fighting continued against forces which had been aligned with the ousted *de facto* government and/or were composed of, or comprised, Al Qaeda operatives. Since actions speak louder than words, the Nations in question have acknowledged – regardless of any public statements their governments may have made later – by way of continuing to contribute these forces with a mandate to support U.S. self-defence, the nature of the armed conflict in Afghanistan as a non-international armed conflict in exercise of the right of self-defence against a non-governmental actor.

287 For a similar assessment see the 'Fourth report on responsibility of international organizations' (UN document A/CN.4/564) submitted to the International Law Commission by Giorgio Gaja, Special Rapporteur, at para 19.

COLLECTIVE SECURITY IN NATO PRACTICE

Collective security within NATO is primarily captured by Articles 4 and 7 of the North Atlantic Treaty. Article 4 establishes the mechanism for consultations concerning threats to the territorial integrity, political independence or security of any NATO Nation. Article 7 specifies that the North Atlantic Treaty:

> 'does not affect, and shall not be interpreted as affecting in any way the rights and obligations under the Charter of the Parties which are members of the United Nations, or the primary responsibility of the Security Council for the maintenance of international peace and security'.

This clause enables NATO Nations to utilise the Alliance in fulfilling any obligations they may have under the UN Charter. – The legal bases just discussed are supplemented by implied powers associated with the North Atlantic Treaty which enable the Alliance to take appropriate action in support of its purposes, in particular collective security and defence of its members.

As will discusses shortly, Article 7 of the North Atlantic Treaty provides an appropriate plug-in point for NATO Nations to leverage the Alliance in fulfilling their obligations under the UN Charter. In particular, this provision confirms that NATO's implied power to launch operations designed to enhance collective security may also be used when such operations coincidentally also support the purposes of the United Nations[288].

The Article 4 mechanism for collective security through consultations does not pose major legal challenges. In the single reported case, the consultations requested by Turkey were conducted in NATO's Defence Planning Committee which on 16 February 2003 requested military advice from NATO's Military Authorities[289] and on 19 February 2003 authorised the implementation of defensive measures[290], namely the deployment of AWACS, Patriot missiles, and other defensive systems[291]. However, it appears that an earlier request to provide NATO support to Turkey met

288 In the practice of the North Atlantic Council, the assessment that NATO and UN purposes converge is usually expressed by way of a reference to the relevant resolution of the UN Security Council. See, for example, the fact sheet concerning the NATO Training Mission in Iraq at http://www.nato.int/cps/en/natolive/topics_51978.htm (last visited 31 August 2010).

289 See the DPC Decision Sheet at http://www.nato.int/docu/pr/2003/p030216e.htm (last visited 29 August 2010).

290 See Press Release (2003)013 at http://www.nato.int/docu/pr/2003/p03-013e.htm (last visited 29 August 2010).

291 See Paul Gallis, NATO's Decision-Making Procedure (CRS Report for Congress, Order Code RS21510, 05 May 2003; online at http://www.fas.org/man/crs/RS21510.pdf (last visited 29 August 2010)), at 2.

resistance – which, however, was not based on legal arguments[292].

On comparison with the thresholds contained in the UN Charter, threats to the territorial integrity, political independence or security certainly comprise any threat or use of force against the territorial integrity or political independence prohibited by Article 2(4) of the UN Charter, and likewise any threat to the peace, breach of the peace, or act of aggression as contemplated by Article 39 of the UN Charter – in both cases specifically when they do not amount to an armed attack[293] on a NATO Nation. Moreover, as indicated by Beckett's discussion of a possible conflict between the Article 4 mechanism and the right to engage the United Nations in case of looming security threats, each NATO Nation may also seek consultations if it finds itself in a 'dispute, the continuance of which is likely to endanger the maintenance of international peace and security' (cf. Article 33 of the UN Charter), provided it is of the opinion that such dispute involves at least an emerging threat to its territorial integrity, political independence or security.

The mechanism for collective security through utilising NATO in fulfilling obligations under the UN Charter is rooted in the link between Article 7 of the North Atlantic Treaty and Article 48 of the UN Charter. Article 48 specifies that 'decisions of the Security Council for the maintenance of international peace and security' (paragraph 1) 'shall be carried out by the Members of the United Nations directly and through their action in the appropriate international agencies of which they are members' (paragraph 2). Whilst the term 'international agency' seems dated from a contemporary perspective, it should be beyond doubt that it is not only capable of covering international organisations such as NATO but also has been

292 As reported, it could have been misunderstood as 'the equivalent of acknowledging that Iraq had impeded U.N. weapons inspections' – which was not proven according to the objecting governments – and might have amounted to a pretext for the impending resumption of hostilities against Iraq. Paul Gallis, NATO's Decision-Making Procedure (CRS Report for Congress, Order Code RS21510, 05 May 2003; online at http://www.fas.org/man/crs/RS21510.pdf (last visited 29 August 2010)), at 1.

293 For the differentiation between the thresholds defined in Articles 2(4) and 51 of the UN Charter, respectively, see the judgment of the International Court of Justice in the '*Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*' – ICJ Rep. 1986, 14-150, at para 210.

applied by the UN Security Council on the basis of this interpretation[294]. It follows that the observation that Article 48 of the UN Charter may contain 'an anticipatory reference to the regional agencies which come under Chapter VIII'[295] should not be misread such as to imply that its scope have to be considered limited thereto[296]. Conversely, Article 7 of the North Atlantic Treaty and Article 48(2) of the UN Charter build a bridge connecting the substantial legal bases for non-self defence action in the said international agreements. The North Atlantic Council has repeatedly used the powers implied in the North Atlantic Treaty to take action enhancing NATO's and its Nations' security, including by way of operations involving the use of force, namely in the form of Non-Article 5 Crisis Response Operations.

As a result, NATO's collective security mechanisms comprise consultations under Article 4 and utilising the organisation's implied powers *inter alia* to coincidentally fulfil its Nations' obligations under the UN Charter. Once again, the interpretation and application of the relevant provisions of the North Atlantic Treaty and the UN Charter, respectively, are in harmony; and the practice in the UN Security Council, the North Atlantic Council, and among the NATO Nations (as well as the States which have contributed forces to NATO-led operations) is sufficiently well entrenched to supplement these relevant provisions.

CONCLUSION AD INTERIM: NATO'S SECURITY POLICY ACQUIS

As indicated by the discussion of the practice regarding NATO's collective security

294 By way of example, the UN Security Council has implicitly referred to NATO as the designated lead organization of the Implementation Force (IFOR) for the Dayton Peace Agreement in Bosnia and Herzegovina in welcoming 'the willingness of the Member States acting through or in cooperation with the organization referred to in Annex 1-A of the Peace Agreement' (see para 12 of UNSCR 1031). The words 'acting through' in this paragraph clearly resemble the phrase 'through their action' in Article 48(2) and should, given the absence of any indications to the contrary, hence be regarded as an indication that the UN Security Council had Article 48 in mind in adopting resolution 1031. – Later resolutions contained express authorisations of NATO *sub specie* 'relevant international organizations' (para 7 of UNSCR 1244 – Kosovo Force (KFOR)) or acknowledged NATO's role as the lead organisation by way of noting relevant correspondence (cf. the eighth and ninth preambular paragraphs of UNSCR 1510 (International Security Assistance Force (ISAF)) concerning the letter dated 10 October 2003 from the Minister for Foreign Affairs of Afghanistan – UN document S/2003/986, annex – which contains the statement that '[t]he Afghan authorities have repeatedly welcomed the assumption of strategic command, control and coordination of ISAF by the North Atlantic Treaty Organization (NATO)' – and the letter dated 06 October 2003 from the NATO Secretary General regarding the expansion of ISAF's mission – UN document S/2003/970).

295 Beckett, at 12.

296 Apart from being counterintuitive, such a limitation of the scope of Article 48 of the UN Charter has no foundation in its language. Speaking of 'appropriate agencies', it does not anticipate the formula used in Article 52 of the UN Charter, namely 'regional arrangements or agencies'. As a result, the criteria under Chapter VIII of the UN Charter are without prejudice to the question of whether 'agencies' – or, in more modern language, international organisations – are 'appropriate' for the purposes of taking '[t]he action required to carry out the decisions of the Security Council for the maintenance of international peace and security'.

and defence mechanisms, NATO has progressively developed a well-balanced security policy *acquis* which adapts the said mechanisms so as to maintain coverage of the whole spectrum of threats the Alliance and its Nations may be exposed to. It does not require much creative thinking to argue that the decisions and practice contributing to this security policy *acquis* 'shall be taken into account' (Article 31(3) of the Vienna Convention on the Law of Treaties) in confirming the appropriate interpretation of the relevant legal bases.

As an integral part of this security policy *acquis*, NATO's repertoire of responses comprises – in addition to any diplomatic means of the Alliance's choice – both the facilitation and/or support of action taken by its Nations individually or in concert, and NATO/NATO-led operations. The latter may coincidentally support the collective security of NATO and its Nations as well as the principles of the United Nations, including as applied to an individual situation by the UN Security Council in a Chapter VII resolution.

The emergence and consolidation of this security policy *acquis* demonstrate the flexibility of the North Atlantic Treaty. Moreover, taking into account the Vienna Convention on the Law of Treaties, they should also be considered to reflect the emergence and consolidation of a legal policy consensus regarding the interpretation and application of the North Atlantic Treaty.

INTEGRATING CYBER SECURITY AND DEFENCE IN NATO'S SECURITY POLICY ACQUIS

Forging a policy consensus concerning the interpretation and application of NATO's legal bases to cyber activities may require taking into account multiple thresholds, including such pertaining to other domains than international law. As discussed earlier, NATO yet has to include collective cyber security and defence in its policy consensus regarding the interpretation and application of its legal bases. To do so, NATO may have to address a range of challenges associated with international law, legal and political policy, and institutional arrangements. Whilst no official communiqué tackles the whole range of these challenges, different aspects thereof are addressed in the experts report and national level policy statements or documents. To date, according to the experts "cyber attacks against NATO systems occur … most often below the threshold of political concern"[297]. This cautious language identifies 'NATO systems' rather than NATO as affected by cyber attacks; it does not discuss NATO Nations and/or their computer and

297 See the experts report, at 45.

communications systems. It is hence without prejudice to assessments made at national level. Indeed, from one or more perspectives the threshold of political concern may well have been crossed more than once. For instance, His Excellency Mr. Toomas Hendrik Ilves, President of the Republic of Estonia, has observed that there have already been cases of actual or prevented aggression against nation-states carried out in cyberspace: "Were they to have been carried out with kinetic weapons, we in NATO would be faced minimally with an Article 4 and most likely with an Article 5 scenario."[298] By contrast, the Federal Government of the Federal Republic of Germany has recently addressed cyber attacks directed from abroad in the 2010 edition of the 'Verfassungsschutzbericht' (covering the year 2009)[299], a report commissioned by the Federal Ministry of the Interior on the basis of police and intelligence reporting which tackles threats to Germany's constitutional order – i.e. significant threats to internal, or homeland, security.

POLITICAL POLICY AND INSTITUTIONAL ARRANGEMENTS

The fact that a given cyber threat or incident crosses the threshold of political concern is without prejudice to its political and legal characterisation for the purpose of developing an appropriate response. Much will depend on political policy perceptions – are cyber threats and incidents predominantly perceived as human rights (i.e. data privacy) issues, matters of law enforcement and/or homeland security[300], or matter of national security and defence – and the different roles played by the government agencies involved on the examination and assessment of cyber threats and incidents, and competent to adopt or contribute to actual responses. Accordingly, it may be for multiple reasons that NATO faces challenges in developing consensus regarding the full integration of cyber security and defence in its respective mechanisms, as well as the necessary institutional arrangements.

First, in an environment where any security and defence discourse is to a great extent predetermined by the level of political concern, there may simply have been a limited number of opportunities to actually put cyber security and defence prominently on NATO's agenda. Second, quite similar to threats arising from international terrorism, threats arising in and out of the cyber space may give rise

298 See http://www.ccdcoe.org/conference2010/329.html; cf. http://www.nato.int/cps/en/SID-B2AD4DE6-E0B91B4E/natolive/news_64615.htm? (last visited 30 August 2010)

299 Verfassungsschutzbericht 2009 (preliminary version), at 307sq; available at http://www.bmi.bund.de/cae/servlet/contentblob/1098014/publicationFile/91389/vsb2009.pdf (last visited 31 August 2010).

300 JP 1-02 defines homeland security as: 'A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur.' Reference is also made to JP 3-28 (*ibidem*).

to both internal, or homeland, and external security concerns, and thus trigger the oftentimes complex delineations of competence between the defence, law enforcement, and intelligence sectors which many NATO Nations have developed into strong checks and balances amounting to a separation of powers *en miniature* within their executive branches of government. Whilst obviously such domestic arrangements lack the capacity to affect the interpretation and application of the North Atlantic Treaty[301], they may nevertheless *de facto* challenge NATO Nations' Defence Ministries' as well as Armed Forces' ability to put cyber security and defence on NATO's policy, concept, and doctrine agendas. To date, no well-entrenched method, structure or process for overcoming this *de facto* challenge – e.g. through involvement of foreign intelligence, homeland security and/or law enforcement stakeholders – exists within NATO. Third, there is a near complete lack of NATO-wide, standardised doctrine for cyber warfare. The resulting absence, amongst NATO Nations, of a militarily agreed and legally cleared (Article 36 of GP I) understanding concerning the means and methods of cyber warfare may also contribute to the lack of political policy consensus. The appetite for engaging in hostilities which might be perceived as potentially involving legally doubtful means and methods of warfare may be limited. Ultimately, the absence of consensus regarding *jus in bello* may thus have repercussions on the likelihood that consensus can be reached concerning *jus ad bellum* as well as collective security and defence.

INTERNATIONAL LAW AND LEGAL POLICY

New technology has met laws of greater age on various occasions. Sometimes its impact was smooth, at other times the integration of new technology in existing legal frameworks failed in light of the absence of appropriate plug-in sockets. These alternatives were also discussed with respect to cyber technology. Ever since the arrival of cyber technology in the armouries the effects of their use has been compared to the effects of kinetic warfare. Over the years, the analysis of cyber warfare revealed that, whilst technically speaking, cyber activities have a direct effect on electrons only, the indirect effects caused by them may entail death or injury as well as damage or destruction. Moreover, the use of cyber technology may impact a nation's governability, i.e. deny its government's effectiveness and push it onto the slippery slope towards destabilisation and failure.

301 See Article 27 of the Vienna Convention on the Law of Treaties.

Following an earlier period of significant discussions of *jus ad bellum*[302] (and *jus in bello*[303]) concerning cyber attacks around the turn of the millennium, the 2007 cyber attack faced by Estonia as well as the use of cyber capabilities in the context of the armed conflict between Russia and Georgia in 2008 have led to renewed interest in matters of cyber warfare. This section will discuss four types of scenarios involving the use of cyber technology from a *jus ad bellum* perspective. It will analyse these scenarios, which are based on an abstraction from examples rather than generic, with a view to establishing whether, as well as in what circumstances and under what conditions, certain usages of cyber technology may be eligible as elements of a (legal) policy consensus regarding NATO's collective security and defence mechanisms.

The first type of scenarios covers the use of cyber technology as an enabler for traditional kinetic force used to launch a campaign. One operation of that nature may have occurred when Israel struck a construction site at Tall al-Abyad, Syria, on 06 September 2007. It appears that the attacking aircraft got through Syria's air defence radars without being detected. According to a report in Aviation Week, an information and service providing business[304], this may have been due to an airborne network attack system which 'allows users to invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen .... The process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading messages algorithms that allow a number of activities including control.'[305] Just like this real world situation, the as of yet theoretical example of a cyber attack disabling

302 The key reference is Michael N. Schmitt, Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Columbia Journal of Transnational Law 885-937 (1999). See also Dimitrios Delibasis, State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century (available at www.peacestudiesjournal.org.uk/dl/Feb%2006%20DELIBASIS.pdf – last visited 31 August 2010).

303 See, for instance, Michael N. Schmitt, Wired Warfare: Computer network attack and *jus in bello*, in: 84 International Review of the Red Cross 365-399 (2002); Steven M. Barney, Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace?, 48 Naval Law Review 43-87 (2001); William Yurcik & David Doss, Internet Attacks: A Policy Framework for Rules of Engagement (available at arxiv.org/pdf/cs/0109078 – last visited 31 August 2010).

304 See http://www.aviationweek.com/aw/About_Us_Home.do (last visited 29 August 2010).

305 See the report 'Why Syria's Air Defenses Failed to Detect Israelis' by David A. Fulghum, posted 03 October 2007; available at http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a2710d024-5eda-416c-b117-ae6d649146cd&plckScript=blogScript&plckElementId=blogDest. This report is quoted at http://www.theregister.co.uk/2007/10/04/radar_hack_raid/ and http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/; a detailed report is available at http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess&channel=defense (all visited 29 August 2010)

the key platform in a ballistic missile launch reporting network[306] would be of a similar nature.

Whilst 'locating enemy emitters' and copying 'what enemy sensors see' are acts of cyber espionage and in that capacity below the threshold of use of force, once the intruders 'take over as systems administrator' – including through 'direct[ed] data streams' – the assessment may change. Any such act of cyber espionage faced by a NATO Nation may, depending on (information and intelligence regarding) the circumstances as well as the relevant strategy and doctrine, amount to a threat of the nature contemplated in Article 4 of the North Atlantic Treaty rather than a mere nuisance. By contrast, seizing control through the use of cyber technology may in itself amount to an illegal use of force and at the same time create a situation where the 'necessity of self-defense [is] instant, overwhelming, leaving no choice of means, and no moment of deliberation'[307]. Exercising control once it has been seized, including by way of manipulating sensors or including false targets, may – again depending on the circumstances as well as the relevant strategy and doctrine – either indicate that an armed attack is imminent, or be an integral part of an actual armed attack.

The second type of scenarios covers hybrid threats of which the use of cyber technology may be one contributing factor. According to a recent conceptual document submitted by NATO's two Supreme Headquarters to the Military Committee, "Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[308] This conceptual approach confirms that 'hybrid threats arise from a blend of simultaneous actions'[309]. The notion of 'blend of simultaneous actions' reflects that in the context of a hybrid threat, weakening NATO and its Nations may be a means to achieve a range of different ends rather than one single strategic objective from the perspective of the adversaries involved. Accordingly, just as adversarial activities contributing to a hybrid threat does not necessarily indicate the existence of any kind of alliance among the adversaries in question, the use of cyber technology as part of such blend does not represent a cyber

306 See the discussion by Thomas C. Wingfield, Legal Aspects of Offensive Information Operations in Space, at 11 (available at www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.doc – last visited 31 August 2010).

307 See Secretary of State Daniel Webster's 'Letter to Henry Stephen Fox', in K.E Shewmaker (ed.). The Papers of Daniel Webster: Diplomatic Papers, vol. 1. 1841-1843 (1983), at 62.

308 BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats (Enclosure 1 to document no. 1500/CPPCAM/FCR/10-270038 – 5000 FXX 0100/TT-6051/Ser: NU0040 dated 25 August 2010 – marked 'NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC'), at para 7.

309 BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats, at para 19.

line of operations. That said, the use of cyber technology in this context would nevertheless either be a multiplier or its effects would be multiplied by any other contributing factor(s). Ultimately, the assessment would depend on the mutually reinforcing effects of the variety of factors capable of contributing to a hybrid threat whose materialisation may amount to an adversary's first strike. Article 5 of the North Atlantic Treaty may be triggered in this context if the scale and gravity of the overall effect of that first strike corresponds with the kinetic equivalent.

The third type of scenarios covers the use of cyber capabilities to degrade or deny decision-making and associated command and control capability, and/or achieve information superiority in the field of strategic communications, both of which may make a significant contribution to campaign success. One operation of that nature may have occurred when armed conflict broke out in Georgia in August 2008. Even prior to the hostilities, a 'short occasion of turbulence' occurred on 19 July 2008[310]. According to unnamed experts, the cyber attacks conducted during the period of hostilities[311] may 'have reduced Georgian decision-making capability, as well as its ability to communicate with allies, thereby possibly impairing the operational flexibility of Georgian forces'[312]. While it seems beyond dispute that Georgia was exposed to cyber attacks, these cyber attacks were assessed from different angles. The Independent International Fact-Finding Mission on the Conflict in Georgia established by the European Union[313] focused on matters of attribution[314] and the novelty of cyber warfare[315] rather than questions of collective security and defence. However, since attribution is a challenge of an overarching nature, it will not be addressed here. By contrast, apparently convinced that attribution was possible in the Georgia case, U.S. Secretary of Defence Mr. Robert Gates has stated in a high level

310 Eneken Tikk *et al.*, International Cyber Incidents (2010), at 69.

311 For the sequence of events see e.g. Eneken Tikk *et al.*, International Cyber Incidents (2010), at 69sq and the September 2009 report of the Independent International Fact-Finding Mission on the Conflict in Georgia, Vol. II, at 218.

312 The September 2009 report of the Independent International Fact-Finding Mission on the Conflict in Georgia observes that some experts believe this (Vol. II, at 217sq).

313 Decision of the Council of the European Union dated 02 December 2008, OJ 2008 No. L 323/66.

314 According to the Report of the Independent International Fact-Finding Mission on the Conflict in Georgia (Vol. II, at 219), 'the nature of defence against cyber attacks at this stage of its development means that such attacks are easy to carry out, but difficult to prevent, and to attribute to a source'. For a detailed analysis of the origin of the cyber attacks on Georgia see Eneken Tikk *et al.*, International Cyber Incidents (2010), at 74sqq.

315 In discussing the (from its perspective: possible) integration of cyber warfare in the hostilities between Russia and Georgia the EU's Independent International Fact-Finding Mission on the Conflict in Georgia observed that, '[i]f these attacks were directed by a government or governments, it is likely that this form of warfare was used for the first time in an inter-state armed conflict'. Report of the Independent International Fact-Finding Mission on the Conflict in Georgia, Vol. II, at 219. It may be noted in this context that, given the absence of reciprocal force, the incident concerning Syria may not have amounted to an armed conflict despite its nature as a use of force which might have constituted an armed attack.

publication that: 'Russia's relatively crude - though brutally effective - conventional offensive in Georgia was augmented with a sophisticated cyber attack and well-coordinated propaganda campaign.'[316] The language used in this assessment seems to be carefully chosen; notably, the cyber attack faced by Georgia was not characterised as either enabling or multiplying the kinetic offensive; yet it was not merely addressed as a sustaining activity, either. As a result, the essence of this assessment may be that the elements carrying out the cyber attack may have been in a supporting rather than a supported role.

Too little is known about the 'short occasion of turbulence' in July 2008 to enable a compelling assessment of its nature from a collective security and defence perspective[317]. However, depending on the circumstances as well as the relevant strategy and doctrine, future 'occasions of turbulence' which affect NATO or one or more NATO Nations might create the impression that an entity acting from abroad is trying to test, or is actually testing, what effects is can generate using its cyber capabilities. If a NATO Nation were affected by such conduct, it would hardly overstretch the collective security mechanism established by Article 4 of the North Atlantic Treaty were it to request consultations with a view to obtaining military advice on the situation.

The Georgia example illustrates that the use of cyber technology may occur in support of a kinetic operation starting a campaign. The key question in this context is how non-enabling usages of cyber technology should be assessed from a legal and legal policy perspective, in particular if they occur prior to the first kinetic strike. One particular question deserving legal policy consensus would concern the circumstances in which 'the risk of a large-scale attack on NATO's command and control systems or energy grids'[318] can be considered to reflect that one or more of NATO's strategic competitors or potential adversaries possess cyber technology whose use can augment their kinetic capability. Information and intelligence regarding the circumstances as well as relevant strategy and doctrine may facilitate related assessments. However, it might nevertheless be more challenging to determine what augmenting usages of cyber technology justify pre-emptive / anticipatory self-defence or self-defence against an imminent attack than making the same determination with respect to enabling usages of cyber technology. At any event, the foregoing is without prejudice to the assessment that an ensemble of

316 Robert M. Gates 'The National Defense Strategy', in: Joint Forces Quarterly, issue 52, 1st quarter 2009, at 1/5.
317 According to reports, the website of the President of the Republic of Georgia was out of service for 24 hours, which may have been caused by a command and control server. See Eneken Tikk *et al.*, International Cyber Incidents (2010), at 69 for references.
318 Cf. the experts report at 45.

effects generated by the use of kinetic means as augmented by cyber technology would most likely cross the threshold of armed attack and hence trigger Article 5 of the North Atlantic Treaty.

The fourth type of scenarios covers the use of cyber capabilities on their own. The main challenge associated with this type of scenarios is tied to the objects affected in such cases, which will usually be civilian rather than military objects[319]. The example mentioned in the experts report concerning 'a large-scale attack on ⋯ energy grids'[320] (assuming for the purpose of analysis that energy supplies for the military are not affected thereby) as well as the cyber attack faced by Estonia in 2007 provide useful points of reference for this type of scenarios. The legal analysis regarding the cyber attack faced by Estonia in 2007 indicates that, from a collective security and defence perspective, this attack did not go beyond the level of a significant nuisance[321]. Even though Article 4 of the North Atlantic Treaty was not expressly invoked, NATO's collective security mechanism proved responsive; according to available reports, consultations were held and capabilities enabling a military assessment were made available. At the same time, the cyber attack faced by Estonia in 2007 as well as the risk of a future large-scale attack on energy grids should be the subject of contingency considerations since it may well be a precursor of what might yet be expected to come. Arguably, the fourth type of scenarios discussed in this paper bears the potential to create the biggest policy challenges NATO may have to tackle.

In a worst case scenario, future cyber attacks may deny one or more governments the ability to govern, or significantly interfere with democratic decision-making at all levels of society and government. For instance, a future cyber attack could significantly affect election results or policy choices. The recent history of the use of kinetic force has demonstrated that such effects may indeed occur[322]; the emergence of electronic government, which may sooner or later involve a 'cyberisation' of

319 Although the notion of 'military object' does not occur expressly in GP I, the differentiation between civilian objects (a notion used in Article 51(1) of GP I) and military objects is an underlying premise of its definition of military objective. Whilst a military object is always also a military objective since it will always fulfil the criteria set out in Article 52(2) of GP I, a civilian object only becomes a military objective if these criteria are met in an individual case.

320 Cf. the experts report at 45.

321 Reportedly, invoking Article 5 of the North Atlantic Treaty was never seriously considered. See Eneken Tikk *et al.*, International Cyber Incidents (2010), at 25sq.

322 The 11 March 2004 and the 07 July 2005 train bombs in Madrid and London, respectively, are ample proof that terrorists can affect the outcome of a general election or legislative priorities and decisions. Cf. my paper 'Air Policing and Counter-Renegade Action: Options beyond the German Aviation Security Act', 48 The Military Law and the Law of War Review 7 (2009) at 55 (text accompanying and footnote 86).

general elections[323], may be accompanied by additional vulnerabilities – which may materialise e.g. by way of identity theft coupled with subsequent use of the stolen identities in eVoting. Likewise, bringing down election servers designated for eVoting may effectively deprive a society of the ability to vote or the election outcome. All these hypothetical challenges have in common that they indicate what target a future cyber attack might be directed at, namely the integrity of the (democratic) decision-making process. Without such integrity, there may be serious doubts as to whether the exercise of the functions of government can still be considered 'effective' for the purpose of attributing relevant acts to any given State as its own sovereign acts[324]. In a similar manner, a future cyber attack could more or less sever the communication links within the government as well as between a government and the society it governs. For instance, interference with such areas of eGovernment as substitute online services for face to face interaction throughout of the administrative branches of various national governments may exploit the fact that sooner or later there will no longer be a workforce that could be mobilised and step in once the bulk of public services is performed based on the use of cyber technology. It may be argued that ultimately a cyber attack of that nature could severely affect the ability of a nation to maintain its political independence or otherwise push a state towards the edge of failure.

Developing a legal policy consensus regarding the best way to address such worst case scenarios from a collective security and defence perspective may require to double check certain well-established legal policy concepts[325]. The range of effects considered to indicate that an armed attack occurs in contemporary law of armed conflict – control of territory and sea access; death and injury; damage and destruction – might turn out to be too closely connected with the parameters of statehood in the 19th and 20th centuries, and hence require innovative adaptation to the realities of the 21st century. The UN Charter's prohibition of the use of force may be worthwhile revisiting for this purpose; namely, the protection of all nations' 'political independence' therein may see a renaissance as a result of a future legal policy discourse. One consideration guiding such discourse could be that it may

323 According to information received from CCD COE staff, Estonia has already introduced internet voting in local government elections. However, it might be worthwhile to not only think about Estonia's fairly advanced eGovernment but also identify equivalent vulnerabilities in other nations, thinking of e.g. the voting computers used in the U.S.

324 See my paper 'Air Policing and Counter-Renegade Action: Options beyond the German Aviation Security Act', 48 The Military Law and the Law of War Review 7 (2009) at 55sq (text accompanying and footnote 87).

325 One such concept is the differentiation between force and coercion for the purposes of applying Article 2(4) of the UN Charter. For a discussion see Matthew Hoisington, Cyberwarfare, the Use of Force & the Right of Self-Defence, 32 Boston College International and Comparative Law Review 439/447sqq (2009).

not make a significant difference whether a nation's political independence is degraded or denied by way of a cyber attack or by way of defeating its armed forces in a kinetic campaign. Ultimately, as Carl v. Clausewitz has observed, '[w]ar is ⋯ an act of force to compel our enemy to do *our will*.'[326] The opposite reverse holds equally true and is point-on in the present context. Within the Alliance, acts designed to impose a foreign actor's political will on a NATO Nation or its society may hence be considered amounting to acts of force – and may accordingly be qualified, for the purposes of international law, as a 'threat or use of force' resorted to in any State's 'international relations' or as an 'armed attack'.

A SPOTLIGHT ON CYBER THREATS CAUSED BY NON-GOVERNMENTAL ACTORS

When explaining the invocation of Article 5 of the North Atlantic Treaty following the 9/11 attack on the United States of America, the North Atlantic Council considered these attacks to possibly having been 'directed from abroad' rather than e.g. 'by another State'. In their reports to the UN Security Council under Article 51, multiple NATO Nations[327] – as well as Australia, following the invocation of the collective self-defence clause in the Security Treaty between Australia, New Zealand and the United States of America (ANZUS) dated 01 September 1951[328] by the Australian Prime Minister and U.S. President on 14 September 2001[329] – expressly mentioned Al Qaeda as one of the entities against which measures were taken in self-defence. No formal objections by members of the UN Security Council or otherwise by any State were reported at the time. This practice indicates that non-governmental actors may be considered responsible for an armed attack, and that self-defence may be directed against them.

Subsequently, questions were raised whether the notion of self-defence against

326 Carl v. Clausewitz, On War, translated by Michael Howard and Peter Paret and published by Alfred A. Knopf in the Everyman's Library series, New York - London - Toronto 1993, at Book One Chapter One Part 2 entitled "Definition" (my emphasis).

327 See the Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council (UN document S/2001/946); Letter dated 7 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (UN document S/2001/947); Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005); Letter dated 29 November 2001 from the Permanent Representative of Germany to the United Nations addressed to the President of the Security Council (UN document S/2001/1103).

328 Available at http://www.australianpolitics.com/foreign/anzus/anzus-treaty.shtml (last visited 03 August 2010).

329 Letter dated 23 November 2001 from the Permanent Representative of Australia to the United Nations addressed to the President of the Security Council (UN document S/2001/1103).

armed attacks carries an implicit limitation which would make the right of self-defence under Article 51 of the UN Charter available only in cases 'of armed attack by one State against another State'. However, the jurisprudence of the International Court of Justice which is usually referred to in support of this position[330] is not undisputed within the court itself. Justice Buergenthal has aptly observed that the majority of the court has taken a 'formalistic approach'[331] in the Advisory Opinion concerning the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory. In DRC v. Uganda, Justice Kooijmans has deplored that in failing to address the question of self-defence against activities of non-governmental actors, the Court 'has missed a chance to fine-tune the position it took 20 years ago' in the Nicaragua case[332], in which Justice Simma has joined him, adding that:

> Security Council resolutions 1368 (2001) and 1373 (2001) cannot but be read as affirmations of the view that large-scale attacks by non-State actors can qualify as "armed attacks" within the meaning of Article 51.[333]

Both Justices have alluded at possible changes of international law in light of practice and refined *opinio juris* in this context[334]. From a legal policy perspective, there is hence room to reinforce the post-9/11 development of practice and to consolidate the *opinio juris* thence refined. It may be noted that Advisory Opinions of the International Court of Justice are indicative rather than binding, and that the judgment in DRC v Uganda has binding force *inter partes* only. Accordingly, NATO and its Nations are not legally obligated to consider the jurisprudence discussed as binding upon them. As indicated by the Article 51 reports submitted in 2001, the perception among NATO nations of what amounts to an 'armed attack' may be broader than the approach taken by the International Court of Justice; nothing prevents them to maintain and reinforce this broader approach as a matter of policy. NATO and its Nations may hence consider it appropriate to take action in individual and collective against armed attacks perpetrated by non-governmental actors which are not attributable to a specific government, and they may consider it equally appropriate to contemplate taking such action against armed attacks perpetrated by non-governmental actors involving the use of cyber technology.

330 The most recent points of reference are the International Court of Justice's Advisory Opinion concerning the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory dated 09 July 2004, at para 139 and its judgment regarding the Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) dated 19 December 2005, at paras 146/147. In essence the ICJ concluded in both cases that activities of armed groups only trigger the right of self-defence if attributable to another State.

331 para 6 (p. 243)

332 Separate Opinion of Judge Kooijmans in DRC v. Uganda dated 19 December 2005, at para 25.

333 Separate Opinion of Judge Simma in DRC v. Uganda dated 19 December 2005, at paras 8 and 11, respectively.

334 Separate Opinions of Judge Kooijmans in DRC v. Uganda dated 19 December 2005, at para 25, and of Judge Simma in DRC v. Uganda dated 19 December 2005, at para 11.

CONCLUSION AD INTERIM: CYBER SECURITY AND DEFENCE FIT IN NATO'S SECURITY POLICY ACQUIS

Questions of attribution aside, the discussion the four different types of scenarios and the specific ramifications of cyber attacks perpetrated by non-governmental actors indicate that nothing in contemporary international law prevents NATO from both fully integrating cyber security and defence in its security policy *acquis* as well as taking appropriate action should the need to do so arise. However, considering also the challenges associated with the lack of a well-entrenched method, structure or process to harmonise the efforts of all relevant stakeholders, developing a solid legal policy consensus on matters of cyber security and defence may amount to a significant effort.

CONCLUSION

The demonstrated flexibility and consensus are fully capable of embracing NATO Nations' individual and collective cyber security and defence, as well. Unless otherwise decided, they may also come to bear with respect to NATO's approach to its own cyber security and defence – both in its Nations' territories and deployed. As demonstrated, the legal framework of the North Atlantic Treaty is sufficiently flexible to enable to Alliance to tackle cyber security and defence. However, as of yet the interpretation and application of the North Atlantic Treaty in cyber matters lacks the policy consensus needed to give a sustainable meaning to an(y) international agreement in its capacity as a policy document. In requiring the Alliance to start developing policy consensus concerning the interpretation and application of Articles 4 and 5 of the North Atlantic Treaty, the experts report 'NATO 2020: Assured Security; Dynamic Engagement' points in the right direction.

As far as the legal contribution to this consensus-building process is concerned, the types of scenarios discussed demonstrate the need for innovative analysis capable of challenging established conventional wisdom. Whilst, as indicated, all usages of cyber technology discussed seem to be eligible for integration in NATO's legal policy consensus concerning collective security and defence, their exact position therein would still have to be determined. This holds true both for legally nested policy development and decisions the Alliance may be called upon to take in the future. Moreover, forging a legal policy consensus on collective security and defence including questions of *jus ad bellum* might be facilitated by parallel concept and doctrine development as well as standardisation in a manner addressing related *jus*

in bello challenges[335]. Borrowing language from the experts report for the purposes of the present conclusion, the question of whether any of the usages of cyber technology discussed 'triggers the collective defence mechanisms of Article 5 [of the North Atlantic Treaty] … will have to be determined by the [North Atlantic Council] based on the nature, source, scope, and other aspects of the particular security challenge'[336].

335 Some of the examples contributing to the four types of scenarios discussed supra are reflected in the *jus in bello* considerations discussed by Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, 106 Michigan Law Review 1427-1451 (2008).

336 See the experts report, at 20.