THE TALLINN PAPERS

A NATO CCD COE Publication on Strategic Cyber Security

HANNES KRAUSE

NATO ON ITS WAY TOWARDS A COMFORT ZONE IN CYBER DEFENCE

Tallinn Paper No. 3.
2014

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Previously in This Series

No. 1 Kenneth Geers "Pandemonium: Nation States, National Security, and the Internet" (2014)

No. 2 Liis Vihul "The Liability of Software Manufacturers for Defective Products" (2014)

Roles and Responsibilities in Cyberspace

The theme of the 2014 Tallinn Papers is 'Roles and Responsibilities in Cyberspace'. Strategic developments in cyber security have often been frustrated by role assignment, whether in a domestic or international setting. The difficulty extends well beyond the formal distribution of roles and responsibilities between organisations and agencies. Ascertaining appropriate roles and responsibilities is also a matter of creating an architecture that is responsive to the peculiar challenges of cyberspace and that best effectuates strategies that have been devised to address them.

The 2014 Tallinn Papers address the issue from a variety of perspectives. Some of the articles tackle broad strategic questions like deliberating on the stance NATO should adopt in cyberspace matters, or exploring the role small states can play in this domain. Others touch upon narrower topics, such as the right to privacy in the growingly intrusive national security context and whether software manufacturers should be compelled to bear their burden of cyber security by making them liable for faulty software. The thread running through all the papers, however, is their future-looking approach, one designed to inspire discussion and undergird strategic development.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

NATO on Its Way Towards a Comfort Zone in Cyber Defence

Hannes Krause[1]

Among other pressing issues the NATO Summit in 2014 will provide the Alliance with an opportunity to review its political principles related to cyber defence. NATO adopted its current cyber defence policy and accompanying action plan three years ago.[2] In some areas its implementation has been publicly announced, thereby suggesting that progress has been made; whereas in other areas visible progress is lacking, suggesting that the organisation may be facing challenges. If NATO truly wants to pursue a collective effort within the cyber realm, which could be anticipated as being its natural comfort zone in cyber defence, its new policy will first have to consider the lessons learnt following the adoption and implementation of the present guidance. The steps it will introduce will have to be gradual and realistic, while still increasing NATO's collective efforts in cyber defence. Against that background, this Tallinn Paper discusses some of the ambitions set out in the 2011 document and certain challenges which NATO and Allies have faced in its execution. It will then offer some realistic avenues for achieving progress. As NATO is renewing its political foundation in cyber defence, the Alliance is hopefully on its way towards creating a comfort zone in cyber defence.

Achievements Since 2011

In 2011 NATO's Deputy Assistant Secretary General, Dr Jamie Shea, commented on the adoption of the (then) renewed cyber defence policy by saying:

> The new NATO policy will not only enable NATO to defend its own networks more quickly and effectively but also provide much more assistance to Allies and Partners in all the three crucial areas of cyber security: prevention, coping with cyber attacks and limiting their impact, and helping countries which are attacked to recover and restore their

1 Assistant Defence Counsellor, Permanent Representation of Estonia to NATO. The views expressed are those of the author in his personal capacity.

2 'Defending the networks: The NATO Policy on Cyber Defence,' available at: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf

vital information systems rapidly.[3]

These articulated ambitions contained some clear ideas where progress was to be achieved. The principal official's comment suggests that in 2011 NATO's activity vector was, to a significant extent, envisaged to be directed outside NATO as an organisation, both towards Allies and even towards third parties.

The track-record of the cyber policy's implementation demonstrates that NATO has achieved some visible success: the governance of its cyber defence activities has improved by becoming more structured, and the Alliance seems to have invested heavily in the defence of its own networks.[4] More specifically, the Cyber Defence Management Board (CDMB) was set up as a coordination body within NATO, and NATO Computer Incident Response Capability's (NCIRC) capacity to detect and handle cyber attacks against the Alliance has been enhanced. Indeed, concentrating on its own backyard first has been the key goal of the existing NATO cyber defence policy. That said, no public evidence of progress in NATO's support to Allies has been presented other than the NATO Secretary General concluding last October that NATO's role could be "useful".[5] Therefore, it is appropriate to ask what has kept NATO from achieving its ambitions and which avenues should it pursue *anno* 2014?

Cyber and Collective Defence

The Lisbon Summit, which resulted in NATO's 2010 Strategic Concept, revealed there was no political confusion over whether cyber attacks against its members could justify them turning to NATO for assistance or invoking Article 5 of the North Atlantic Treaty. This is in line with NATO's traditional pattern of thinking, which has always revolved around collective action and response. The challenging question here is practical in nature rather than one of principle: how could and should NATO support its Allies in a cyber-crisis, whether at the Article 5 level or below, taking into account all the features of the cyber domain?

A relatively easy and very NATO-like solution would be to create a commonly funded capability that all Allies could rely on to a certain degree. In fact, in 2011 NATO commenced work on a Rapid Reaction Team concept in which cyber

3 'Cyber defence: next steps,' (10 June 2011), available at: http://www.nato.int/cps/en/natolive/news_75358.htm?selectedLocale=en

4 'NATO and cyber defence,' available at: http://www.nato.int/cps/en/natolive/topics_78170.htm

5 'NATO Defence Ministers move forward with Connected Forces agenda,' (22 October 2013), available at: http://www.nato.int/cps/en/natolive/news_104241.htm?selectedLocale=en

defence experts would be deployed to assist a member state in the event that a cyber attack of national significance had taken place.[6] However, either the Rapid Reaction Team concept has not received unanimous support within the Alliance, or progress has stalled for some other reason. It may well be that the uniqueness of cyberspace significantly hampers this solution's practicability when compared to a traditional military context in which NATO is comfortable operating. For example, the Rapid Reaction Team would first need time to acquaint itself with the targeted information systems, but in the face of an on-going cyber attack action must be taken as quickly as possible. Therefore, alternative and more flexible solutions for cooperative or collective cyber defence should perhaps be considered.

A middle-ground option would be to foresee a facilitator or a coordinator role for NATO, instead of it serving as the provider of direct assistance. Keeping in mind that even in conventional domains NATO routinely commands fairly limited capabilities, the same logic should probably be applied to the cyber domain. Instead of assisting member states itself, NATO could try to play a useful intermediary role in the assistance – whatever shape or form it takes – that Allies provide to each other, both in times of crisis as well as when they are working preventively or recovering from attacks. However, even in this case "cyber" will to an extent challenge the conventional thinking pattern.

An issue of critical importance is knowledge of other states' capabilities and skill-sets. Such information is usually shared bilaterally between nations that have established trust-based relationships, and most probably not via any intermediary. Although some states have revealed limited information about national capabilities,[7] nations undertaking any serious cyber capability development are unlikely to share substantial information about that process with the Alliance.[8] This is an important obstacle for the time being, and needs to be borne in mind as such in all political considerations.

6 'NATO Rapid Reaction Team to fight cyber attack,' (13 March 2012), available at: http://www.nato.int/cps/en/natolive/news_85161.htm?selectedLocale=en

7 Over 30 countries are said to have both the capabilities and the doctrines to conduct offensive operations in the cyber domain – Nigel Inkster, 'Snowden – myths and misapprehensions,' *Politics and Strategy: The Survival Editor's Blog* (15 November 2013). These include, for example, the United States (see, e.g., Ellen Nakashima, 'Pentagon to boost cybersecurity force,' *The Washington Post* (28 January 2013)), the Netherlands (The Defence Cyber Strategy, p. 11), France (White Paper. Defence and National Security 2013: Twelve key points, p. 6) and the United Kingdom ('New cyber reserve unit created,' (29 September 2013), available at: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit).

8 See also Julianne Smith, 'NATO Must Get More Serious on Cyber Security,' *Chatham House Expert Comment* (6 February 2014), available at: http://www.chathamhouse.org/media/comment/view/197236.

Using NATO's Defence Planning

The core of NATO's activities has always been the military cooperation between its member states that predominantly takes the form of joint military operations and campaigns, or collective defence of NATO territory. Such activities are enabled by the defence planning process, designed to primarily ensure that Allies have all the necessary means in their inventories for such cooperation. Therefore, in principle, the defence planning process could also encourage Allies to invest in cyber defence.

The precondition for an effective use of the defence planning process in cyber defence is not only information about existing capabilities, but also differing national policy, legislative and doctrinal approaches. While today it is natural to imagine NATO asking its members to invest in armoured capabilities or transport planes, it is not so easy with respect to cyber capabilities. For the latter to materialise there is clearly a need for more openness on cyber matters, particularly on national capabilities.

NATO's need for secure national infrastructures, interoperable cyber defence capabilities, and for the integration of cyber defence considerations into its operational thinking, is even more relevant in 2014 than it was three years ago. Therefore, a political effort should be made to employ NATO's sophisticated and well-established defence planning process also in the cyber context. Since the overarching goal of the defence planning process is to bring together the civilian and military aspects of Allied defence, there is no reason to rule out its application to cyber capability development. Consequently, cyber defence should become a normal domain of planning and discussion in NATO.

Information Sharing

Sharing information is a precondition for many possible avenues of progress for NATO in cyber defence. Encouraging Allies to use NATO as a channel for information sharing would serve as a good political starting point for further cyber defence discussions within the Alliance, and information sharing should be set as one of the political goals of NATO's cyber defence policy. This could include information related to situational awareness, national developments and existing capabilities.

Without a broader willingness and framework in which to share information, NATO will be severely impeded in its ability to play a more sophisticated role within the cyber domain. However, information will only start to flow if this is

set as a political goal in the new cyber defence policy. It can be assumed that a more liberal stance towards transparency will not only enhance the knowledge-base of all participants, but enable the design of a meaningful organisational action plan for the Alliance's cyber defence.

Cyber Defence Exercises

Another building block for shaping NATO's precise role in collective cyber defence that could also potentially curtail the reluctance to make advances in information sharing is cyber defence exercises. Although easily overlooked, their significance is definitely greater than it may seem at first glance. For six years NATO has conducted an annual dedicated cyber defence exercise called "Cyber Coalition", which has steadily grown both in size and sophistication.[9] Similarly, many Allies and partners regularly participate at the NATO Cooperative Cyber Defence Centre of Excellence's annual Locked Shields exercise series in Tallinn.

At this point in time, NATO should take a serious look at its cyber exercise needs across the Alliance, and match them with the available possibilities and concurrently facilitate possibilities for more exercises based on the needs of its member states. In this context, the Estonian offer to NATO to use its national cyber range as the Alliance's cyber defence training field, including its use in exercises, should not be overlooked.[10] In addition to defining and advancing its specialised cyber exercises, NATO should ensure that its military exercises also incorporate cyber defence elements. As recent history has shown, cyber operations play an important role in contemporary political-military conflicts, with tangible implications for NATO.[11] Therefore, any exercise designed to increase the preparedness for modern conflict should also take the cyber domain into account, both in its planning and execution phases.

While focussed on the practical cyber defence challenges and ways to address them, NATO should not underestimate the political ramifications of advancing its cyber defence exercise programme. Obviously, participants will acquire a better understanding of each other's capabilities and skill-sets through regular

9 'NATO holds annual cyber defence exercise,' (26 November 2013), available at: http://www.nato.int/cps/en/natolive/news_105205.htm.

10 'NATO Secretary General thanks Estonia for offer of cyber range,' Estonian Ministry of Defence (16 February 2014), available at: http://www.kaitseministeerium.ee/en/nato-secretary-general-thanks-estonia-for-offer-of-cyber-range.

11 Adrian Croft, Peter Apps, 'NATO websites hit in cyber attack linked to Crimea tension,' *Reuters* (16 March 2014).

exercises, as is the case with all collective exercises. In cyber defence, such exercises would also result in closer personal relationships, thereby facilitating information sharing at the working level. These, in the long run, build trust-based solid institutional relationships, which are a precondition for any collective approach to cyber defence.

NATO's Potential Focal Points *Anno* 2014

For NATO to realise its full potential within cyber defence it needs to start taking the gradual and realistic steps described in this paper, whilst not shying away from a more active approach towards cyber defence. With several of its members either overtly or covertly developing, and even declaring, their offensive cyber capabilities, whether military or non-military, NATO cannot stand silently by as a matter of principle.[12] Indeed even having this discussion is clearly an element of applying the principle of collective defence in the cyber realm. Looking at 2014, reaching the possible starting-point for this debate actually depends on successfully taking the first steps in information sharing, defence planning and cyber exercises as described above. It is clear that only small and gradual steps will take NATO closer to its anticipated cyber defence comfort zone.

12 NATO's 2011 cyber defence policy is strictly defensive and does not foresee the Alliance engaging in offensive cyber operations.