Briefing Paper

Published by the Center for Asymmetric Threat Studies (CATS) **June 2016**

Challenge for NATO – Cyber Article 5

Jarno Limnéll, Professor of Cybersecurity, Aalto University, Finland
Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs

Invoking collective defense may not have to involve physical destruction. It is time for NATO to rethink how Article 5 is interpreted.

NATO members have declared cyber as an operational domain, just like air, see and land. The decision reflects a notable adaptation in the Alliance's 67-year history, and can be seen as part of a broader move to adapt the alliance to changing warfare and security needs. In doing this, NATO members have agreed to defend against attacks in cyberspace just as they do against attacks launched against targets on other warfare domains. NATO is adapting to its cumulative dependence on the digital domain and responding to the increasing sophistication of cyber capabilities developed by state and non-state actors. The cyber domain is acknowledged to be an integral part of today´s modern wars, conflicts and crises, and more specifically NATO´s current and future operative security environment.

Cyber is becoming an inseparable part NATO's fundamental principle of collective defense. The need for ambitious decisions in the Warsaw Summit and beyond is driven forward by the accelerating threat and increasing questions over resilience of networks upon which daily life has come to depend. Incorporating cyber into other activities, clarifying the cyber policy with regard to Article 5 and readiness to conduct full-spectrum cyber operations with shared capabilities are not just a wish for NATO - they are a necessity in today´s dynamic, complex and uncertain world.

The declaration of cyber as a domain of warfare means that cyber-attacks can more easily be used to justify invoking the collective defence clause - article 5 - of the North Atlantic Treaty. The declaration also reminds NATO member-states that collective cyber credibility begins with countries´ own cyber defenses, which needs to be strengthened. Article 5 specifies "an armed attack" and NATO is officially ready to consider cyber-attacks as an armed attack.

CATS
Center for Asymmetric Threat Studies

SWEDISH DEFENCE UNIVERSITY

A preliminary step in this direction was taken at the Wales Summit two years ago, when NATO declared that a "decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic council on a case-by-case basis." The declaration clarified that the invocation of Article 5 would be conditioned to each single cyber-attack. However, any kind of cyber-attack against a state is a type of aggression. The declaration opens the way for members to take action against the aggressor, including the use of armed force, to restore security.

One of the consequences of this new step is that the Alliance will have to develop a comprehensive cyber doctrine as a separate entity, as well as integrate it into overall planning and strategy documents. Though easy on the surface, it will require NATO to address a number of questions, while acknowledging that the most binary of domains (cyber) is ultimately also one of the more political ones – leading to the concept of cyberpolitics. With the creation of cyberspace, a new arena for the conduct of politics is taking shape, and we may well be witnessing a new form of politics in NATO. The ubiquity, fluidity, and anonymity of cyberspace have already challenged such concepts as deterrence, national security and diplomacy in the traditionally state-centric arena of international relations.

Whatever the shape of the doctrine, whether public or secret, when a cyber-attack occurs in the future and NATO is involved, the doctrine will have to provide reasonable guidelines when satisfactory answers are sought to the following questions:

Who did it? Attributing cyber-attacks to their sponsor remains a significant challenge, especially if attribution is to be public and one-hundred percent certain. The trend is also towards governments outsourcing cyber operations to non-state actors.

What were the consequences of the attack? The speed and covert nature of cyber-attacks makes it difficult to readily establish their magnitude and consequences; moreover, are secondary or tertiary effects to be included in the estimate of consequences?

What are the instruments to respond? And, what is a proportional response? Because cyber capabilities will continue to be primarily national, it is possible that some member states could respond symmetrically, while others must consider asymmetric responses. This is a question of the levers of national power at a state's disposal and willingness to use them. The judgement on proportionality is a political judgement, as it will require a more flexible and historically context aware judgement than a IF-THEN statement in code.

There's also a possibility that when a cyber-attack occurs a member-state may overreact. Political prudence is needed, even though a successful public cyber-attack that is attributed to specific actors would likely create significant political pressure to respond. Restraint should be encouraged, but based on the emerging "cyber warfare playbook" this may be quite challenging.

What then might lead to cyber-attack causing Article 5 to be invoked? No one knows, as it is situationally dependent. The old way of thinking is that a 'severe cyber-attack' has to involve physical destruction – people have to die and physical damage must be seen in the critical infrastructure. However, as we become ever more dependent on data and 'non-kinetic assets', could for example the manipulation of health records lead to Article 5 being invoked? Moreover, is there a difference between banking data and health-care data being manipulated, with one potentially leading to severe economic disruptions and the other in extremis to death.

Formulating clear doctrines is frequently preferred by militaries, while politicians and diplomats prefer flexibility in message and response. The Alliance has two paths it can chose in creating the doctrine regarding cyber. It can either chose a public approach, rather similar to its approach when creating its most recent strategic concept. In such a document it could generally describe what constitutes an attack that would qualify for the invocation of Article 5, and what would be an accepted retaliatory action. The other path is to maintain strategic ambiguity, recognizing that formulating clear redlines would invite potential adversaries to push up to the red line. In this case developing the doctrine is still important, but would then be for internal use only. This non-public approach may reduce the objective of improving the Alliance´s cyber deterrence. The pace of development in the field would argue against an overly specific set of guidelines or doctrine, lest it require too frequent and politically challenging updates.

The current 'cyber warfare playbook' is still a slim volume - but it is growing by the day. In order to remain a credible defence alliance, NATO must possess a credible cyber policy, including cyber deterrence. Credibility comes from a largely similar set of actions as NATO has engaged in regarding conventional military. Doing it in

the cyber domain is, however, harder at the moment. For example, what is the equivalent of standing up in practice permanent battalions in member states? How do you exercise, publicly message determination to defend and counter aggression, in a serious but non-threatening way?

NATO has to find a clear way to deal with a 'Cyber Article 5' event. It may be necessary to reinterpret what Article 5 and an armed attack constitute in today´s world. The biggest challenges is to reach a shared understanding of the limits (physical and cyber) which could lead a member state to invoke Article 5 and delineate what proportionality in response means. The decisions are political by their nature and requires strong understanding on strategic cyber domain and its development by the political actors involved. Ultimately, success will depend on how the cyber is blended with traditional political and military power.

The Center for Asymmetric Threat Studies (CATS) at the Swedish Defence University is a national research center with the task to develop and disseminate scientific and policy-relevant knowledge on asymmetric threats.

This series of occasional briefing papers are published together with our national and international partners on timely subjects within CATS´ areas of interest.

Swedish Defence University
P.O. Box 27805
SE-115 93 Stockholm
www.fhs.se/cats

CATS
Center for Asymmetric Threat Studies

SWEDISH DEFENCE UNIVERSITY