NUPI Norwegian Institute of International Affairs

Policy Brief
[1 / 2019]

Military Offensive Cyber-Capabilities: Small-State Perspectives

Lilly Pijnenburg Muller

Summary

This Policy Brief provides an overview of the military cyber-defence strategies and capabilities of Norway and of the Netherlands. Comparison of the two different approaches offers insights into their differing tactics and future policy directions. The Brief contributes with a small-state perspective on this malleable and constantly changing field, nuancing the hitherto US-centred debate on the utility and need for deterrence and defence in cyberspace.

A common refrain about fighting in cyberspace is that the offence has the advantage over the defence.[1] The offence needs to be successful only once, whereas the defence must be perfect all the time. This has led to offensive cyber-operations being seen as entailing significant strategic advantages for state actors, serving as force multipliers as well as independent strategic assets.[2] Yet, questions remain unresolved regarding the military resources and efforts necessary for conducting such operations.

To discuss what offensive capabilities the military needs, we must first clarify its current scope and role. As noted by Michael Sulmeyer, much of cyber-defence is about situational awareness of one's own assets and capabilities.[3] The debates and empirical studies on cyber defence and deterrence to date have been largely US-centred. However, matters of defence and deterrence are not just a great-power issue. To nuance the debate, this Policy Brief offers an overview of the role and operational capabilities of two medium-sized NATO member-countries, Norway and the Netherlands, as regards to their efforts to build defence in cyberspace.

A major challenge in the study of cyber-defence is that most of what happens in that sphere is conducted in secret. Military missions integrate offensive and defensive operations to achieve and maintain the desired degree of cyberspace superiority, but public statements have been limited. There is a difference between using offensive capabilities in military operations in war, and their use in peacetime – beyond espionage. The first has become a given in our times; the second is controversial. A balance needs to be struck.

This brief is based on public statements and open-source government documents on the defence capabilities and strategic goals of Norway and the Netherlands. Complemented by interviews, it compares these two countries' military positions towards cyber-defence, their stands on offensive capabilities, and their current national military resources and efforts to achieve these. This study of the approaches chosen by these two countries for tackling the challenges ahead, sheds light on how their defence cyberspace strategies are moving in different directions and illustrates that there is no one right way to build defence and deter in cyberspace.

Norway and the Netherlands: defence of the cyber domain

Norway

In Norway, the military plays a limited role in cyber-defence: it is primarily concerned with the protection of its digital systems through the Norwegian Armed Forces Cyber Defence. In other words, the military is to defend its *own* ICT systems within a broader definition of securing national cyberspace.

The offensive side of the Norwegian cyber-security posture is not articulated in detail. According to the 2012 long-term plan for the Norwegian Armed Forces, the external Norwegian Intelligence Service (NIS) is to have the ability to 'conduct both offensive and defensive operations'.[4] In the 2016 revised long-term defence plan, the 2012 phrasing is toned down even further: NIS capabilities are here vaguely formulated as the ability to gather intelligence independently in the cyber-domain.[5] According to the proposed revised law for NIS (currently subject to an open hearing), NIS is to be mandated to conduct offensive cyber-operations, as well as having national responsibility for planning and conducting such operations.[6] Operations are to be consistent with international law, but the legality of each situation is to be assessed, and an operation may be initiated in peacetime in response to an 'international wrongful act' by a foreign state actor.

While little is specified beyond this, both the internal and external intelligence services (PST and NIS) have in recent years made it clear, through annual reports and public statements, whom they view as threat actors in the digital domain. The Ministry of Defence (MoD) holds that, by going public about whom it sees as threat actors, it is also being open about its capabilities within the intelligence organization. Through communicating whom it sees as threat actors, it aims to communicate its own awareness, knowledge and ability to defend against these actors. While this may appear to indicate a slightly more assertive stance, the Norwegian posture in general has remained restrictive, and any offensive capabilities are not publicly signalled or referred to.

The Norwegian military strategy for defending cyberspace is in this way seen to follow the broader national approach to prioritizing resilience, understood as the ability to 'bounce back' from serious cyber-events and to ensure damage limitation.[7] The government recognizes the importance of including the military in securing cyberspace, but has been reserved in public statements on the matter or any further clarification of the role of the Norwegian state in cyber-defence. Other recognition of a broader defence posture in cyberspace as announced in government reports, strategies or publications has been scarce. Thus, Norway seems to take a restrained position as regards the role of the military in cyber-defence, focusing on resilience.

The Netherlands

The Dutch Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV), advised the government of the Netherlands publicly about 'cyber warfare' for the first time in 2011.[8] Their Cyber Warfare Report AIV/CAVV. No 77 concluded that the armed forces are to have the core tasks of 'defending national and allied territory; protecting and promoting the international legal order and international stability',[9] and that the 'deployment of operational cyber capabilities should facilitate these core tasks'.[10] Further, according to the report, t '[o]ffensive cyber capabilities can be deployed in military operations'.[11]

Following the AIV and CAVV recommendations, the government of the Netherlands stated publicly that offensive cyber-capacities should become a regular part of the overall military capability of the country's armed forces.[12] Offensive cyber-capabilities under the Dutch cyber-command have been developed within the armed forces, alongside the creation of a cyber-doctrine and a cyber-strategy.[13] As to the latter, the government acknowledged cyberspace as 'a fifth domain', and stated that cyber-capacities would increasingly become an integral part of military action. It concluded that the ability to conduct offensive cyber-operations was of paramount importance to ensuring the effectiveness of the country's armed forces.[14]

Various measures have been taken to integrate cybersecurity in the Dutch military. The first of these was the implementation of a Cyber-Command within the armed forces, tasked with developing and deploying offensive cyber-capabilities. At its inauguration, the cyber-command was instructed to be capable of deployment during military operations with offensive purposes, like disrupting or disabling the digital networks of an opponent.[15] In 2017 the forces became fully operational; it has claimed to possess specific potential offensive cyber-capabilities, which it also claims never to have employed.[16] In a press statement, the Ministry of Defence has announced that its Cyber-Command can be deployed for offensive tasks, 'such as disrupting or disabling enemy networks and systems such as phones and computers, but also weapon or fuel systems or aircraft altitude meters'.[17]

The Netherlands is open about its offensive capabilities, both generic low-potential and specific high-potential, but has refrained from giving the specifics of capabilities.[18] According to the 2013 Dutch Defence Doctrine, offensive digital operations or digital attacks [are intended to] 'target the enemy's digital systems and information'.[19] The Ministry of Defence's Cyber Strategy goes a step further as to the details, describing offensive cyber-capabilities as digital means for influencing or obstructing the opponent's actions by infiltrating computers, computer networks, and weapons and sensor systems, so as to influence those systems or the information in them. Those means range from easy-to-build measures with a tactical impact, to complex once which are under development, that with a greater strategic impact.[20]

Overall, the Dutch government can be said to take an offensive stand, publicly announcing its offensive military cyber-capabilities. Media reports have made it clear that this entails being active in cyber-operations against other countries.[21] This posture combines the government's understanding of cyberspace as a mature operational domain for waging conflict, and also as a space for preventing it.[22]

Similar defence goals, different strategies?

Norway and the Netherlands have similar outlooks on the challenges concerning threats in and from cyberspace for future cyber-conflict, but differ in their approaches as to how to solve these threats. Both countries recognize the need for offensive capabilities: they vary in how they publicly recognise these, their type and scope.

While the Netherlands is open about its offensive capabilities, activities and goals, the Norwegian government is more restrained in its claims. The government of the Netherlands is vocal about its aim of preventing conflict in cyberspace through offensive means: this is reflected in its development of cyber-offensive capabilities as a defence mechanism; statements that it holds offensive cyber-capabilities, both generic low-potential and specific high-potential; and by stating that it has plans to develop these further.[23] In contrast, the Norwegian focus is on counter-intelligence operations. The Norwegian government and military have limited themselves to minimal public pronouncements concerning their cyber-defence capabilities – in stark contrast to the Netherlands, which has stated its offensive capabilities publicly, without, however, going into detail as to exactly what these capabilities are. Thus, despite having similar goals, the Netherland and Norway differ in their actions regarding their strategies.

The Netherlands and Norway differ in organizational skills and history within their militaries, as reflected in their respective development of cybersecurity policy and strategy. The practice of offence may assume various forms, through cyber-weapons meant to destroy, and espionage. However, there is a difference when such offensive capabilities are used in military operations in wartime, and their use in peacetime (beyond espionage). Whereas the first has become a given in our time, the second remains controversial. Further clarification is called for regarding their differing uses in the grey zone between war and peace. Instead of focusing solely on the utility of offensive cyber-weapons and defence, what we need is a more nuanced picture of the aim of such weapons, and what the offender can achieve by using them.

Most scholars and policymakers claim that cyberspace favours the offense; a minority among scholars disagrees. Such sweeping claims about the offense–defence balance, or arguments for solely defence or solely deterrence are misguided.[24] Both military defence and deterrence capabilities are needed in the cyber-domain, and the balance between the two must be assessed with respect to specific organizational abilities, institutional capacities and technologies.[25]As the cases of Norway and the Netherlands show, there are several ways to achieve this goal, and each country must build on its own internal capacity. Rather than streamlining defence and deterrence, this diversity of approaches is itself a strength.

Examination of the positions of Netherlands and Norway towards cyber-defence and offensive capabilities sheds light on their current national military cybersecurity defence postures. Comparison of the offensive capabilities and strategies of these two small countries provides indications of how they aim to handle the challenges ahead and where their defence cyberspace strategies are moving. The Netherlands and Norway are recognized as two of the most advanced NATO countries with regard to connectivity and cyber-capabilities, but they differ in the balance and use of military capabilities within this sphere.

It should be acknowledged that there is no single, correct way to build defence in cyberspace. The small-state approach and perspectives assessed here can make central contributions to the further development of this increasing important field.

Endnotes

1. Slayton, Rebecca (2017) What Is the Cyber Offense–Defense Balance? Conceptions, Causes, and Assessment, *International Security*, vol 41 (3): 72–109

2. Smeets, Max (2018) The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, 2 (3): 90–113.

3. Sulmeyer, Michael (2018) How the U.S. Can Play Cyber-Offense. *Foreign Affairs*. 22 March, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense

4. Proposisjon 73S 2011-2012: Et Forsvar for vår tid. https://www.regjeringen.no/no/dokumenter/prop-73-s-20112012/id676029/sec3?q=offensive#match_1

5. Proposisjon 151S 2015-2016:Kampkraft og bærekraft, https://www.regjeringen.no/no/dokumenter/prop.-151-s-20152016/id2504884/

6. Ministry of Defence: Høringsnotat – Forslag til ny lov om Etterretningstjenesten https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?expand=horingsnotater

7. Norwegian National Cyber Security Strategy (2012) *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-strategy-for-information-security*

8. Cyber Warfare Report AIV/CAVV. No 77. December 2011, available at http://aiv- advies.nl/6ct/publications/advisory-reports/cyber-warfare

9. Cyber Warfare Report, p. 13

10. Ibid.

11. Cyber Warfare Report, p. 17

12. Response of the Netherlands government to the AIV/CAVV advice on Cyber Warfare. DVB/VD-39/12, of 6 April 2012, available at http://aiv-advies.nl/68w/publicaties/adviezen/digitale-oorlogvoering#government-responses

13. Response (2012) of the Netherlands government to the AIV/CAVV advice on Cyber Warfare DVB/VD-39/12.

14. Netherlands government to Parliament, 27 June 2012, available at https://zoek.officielebekendmakingen.nl/kst-33321- 1.html

15. Netherlands Ministry of Defence (2016) 'Defensie Cyber Commando begin volgend jaar operationeel' Newsletter. 30 November 2016, available at https://www.defensie.nl/actueel/nieuws/2016/11/30/defensie-cyber- commando-begin-volgend-jaar-operationeel (Dutch only)

16. Netherlands government letter to Parliament on offensive cyber-capabilities (2011). 26 643 Informatie- en communicatietechnologie (ICT). Nr. 220 letter from the Minister of Security and Justice, 23 December 2011, available at https://zoek.officielebekendmakingen.nl/kst-26643-220.html and Dutch Ministry of Defence (2016) 'Defensie Cyber Commando begin volgend jaar operationeel'

17. See government letter to Parliament about offensive cyber-capabilities (2011) and Dutch Ministry of Defence (2016) 'Defensie Cyber Commando begin volgend jaar operationeel'

18. H. Vijver (2017) *Deterrence in cyberspace - An analysis of the deterrent use of the Netherlands' offensive cyber capabilities.* MA Thesis submitted to the Faculty of Military Science of the Netherlands Defence Academy.

19. Netherlands Defence Doctrine (2013). Available at: https://english.defensie.nl/topics/doctrine/defence-doctrine.

20. This stance is similar to the UK's national cyber-security strategy, which includes a comparable definition of offensive cyber-capabilities: 'intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction (...) for both deterrence and operational purposes'.See: Ministry of Defence (2015) Letter to the Parliament on the Netherlands' Defence Cyber Strategy Actualization, 23 February 2015. Available (in Dutch) at https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/02/23/kamerbrief-over- actualisering-defensie-cyber-strategie/kamerbrief-over-actualisering-defensie-cyber-strategie.pdf

21. See M. Smeets (2018) The Netherlands just revealed its cybercapacity. So what does that mean?, Monkey Cage Analyses, Washington Post, 8 February https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/?noredirect=on&utm_term=.0795c31787aa; Hogeveen, B. (2018) A rare insight into cyber espionage: Dutch intelligence and two Russian bears, The Strategist, ASPI. https://www.aspistrategist.org.au/rare-insight-cyber-espionage-dutch-intelligence-two-russian-bears/

22. Next to anticipation, deterrence, protection, intervention, stabilization and normalization. See Ministry of Defence report *Verkenningen: Houvast in een onzekere wereld* (2010, Dutch only), p. 197. https://www.defensie.nl/downloads/rapporten/2010/03/29/eindrapport-verkenningen-2010

23. Ministerie van Buitenlandse Zaken (2017) Wereldwijd voor een veilig Nederland – Geïntegreerde Buitenland – en Veiligheidsstrategie 2018–2022.

24. Slayton (2017) op.cit.

25. Ibid.

Norwegian Institute
of International
Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, 0130 OSLO, Norway
www.nupi.no | post@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

Lilly Pijnenburg Muller is a PhD candidate in War Studies, King's College London. She has previously worked as a Research Fellow at NUPI and the Global Cyber Security Capacity Building Centre at the University of Oxford. Her research focuses on cybersecurity, global security practices, international institutions, public–private relationships and risk/threat construction.