Research Division
NATO Defense College

NDC POLICY BRIEF
No. 10 – May 2020

NATO's needed offensive cyber capabilities

Ion A. Iftimie *

At the 2016 NATO Summit in Warsaw, cyberspace was recognized as an operational domain in which NATO military forces must be able to maneuver as effectively as they do on land, at sea and in the air. Since then, Allies have conducted several successful offensive cyber operations[1] against non-state adversaries, such as Daesh. Due to technological transformations in recent years, cyber is no longer viewed by NATO and its member states only as a hybrid threat, but also as a weapon in its own right and as a force multiplier[2] in current military operations. Over the next two decades, NATO will look for new ways to integrate cyber weapons (or offensive cyber capabilities) into its operations and missions.[3]

This *Policy Brief* looks at the distinctions between cyber as a hybrid threat and cyber as a weapon, from theoretical, policy and practice perspectives, and proposes new ways in which NATO can integrate offensive cyber capabilities into its operations.

Cyber as a hybrid threat to, and enabler of, military operations

All future military confrontations are expected to be fought with cyber weapons. These offensive cyber capabilities in the hands of adversaries pose a significant threat to the military forces and critical infrastructure of NATO member states; and the Alliance recognizes that cyber-attacks (as hybrid threats) can be as damaging as conventional ones. This is because malicious cyber activities against computers that control physical processes can be as dangerous as threats that are purely physical in nature and could lead to explosions, nuclear meltdowns, blackouts, or financial crises. As put by NATO Secretary General, "in just minutes, a single cyberattack can inflict billions of dollars' worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and cripple our military capabilities".[4]

All future military confrontations are expected to be fought with cyber weapons

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance's logistics and forward operations. NATO's commitment to "operate and defend itself"[5] in the cyber domain as effectively

* Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business.

1 Offensive cyber operations refer here to coordinated actions where adversary data used to communicate between physical (hardware), logical (software) and/or social (digital persona) systems is infringed upon for the purpose of achieving a specific military effect.

2 J.N. Mattis and F.G. Hoffman, "Future warfare: the rise of hybrid wars", *Proceedings*, Vol.131, No.11, 2005, pp.18-19.

3 D.F. Reding and J. Eaton, *Science & technology trends 2020-2040 exploring the S&T edge*, NATO Science & Technology Organization, Paris, March 2020, p.57, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (accessed on 4 May 2020).

4 J. Stoltenberg, "NATO will defend itself: the Alliance will guard its cyber domain – and invoke collective defence if required", *Prospect*, October 2019, p.4.

5 *Ibid.*

as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance.

Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.[6] Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just to win future wars, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure.

Compared to the air, land and sea domains, the cyber domain is not constrained by national borders

NATO's adversaries in the cyber domain

Warfare in the cyber domain is already conducted against NATO member states by both state and non-state actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary. Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO's current and/or potential future adversaries.

State adversaries in the cyber domain include Russia, China and/or Iran. These are countries known to be building offensive cyber capabilities specifically for the purpose of using them against NATO member states.[7] In Russia's case, cyber attacks were conducted against the critical infrastructure of NATO member states and partner nations, as for example against US energy infrastructure in 2017 (including against a nuclear powerplant near Burlington, Kansas)[8] or against the Ukraine power grid in December 2015. China has also been conducting persistent cyber espionage using offensive cyber capabilities against core military and critical infrastructure of NATO member states for years. For this reason, the US Secretary of Defense, Mark T. Esper, remarked at the 2020 Munich Security Conference that the 5G Huawei infrastructure is a serious threat to NATO.[9] Lastly, Iran's offensive cyber capabilities have also been observed during multiple attacks against the critical infrastructure of NATO partner nations in the Middle East.

NATO adversaries in the cyber domain also include non-state actors, such as terrorist organizations. The US and the UK have conducted several successful offensive cyber operations against those entities. These offensive cyber operations had a significant force multiplier effect, in conjunction with conventional actions on the ground, at sea, in the air and from space, that contributed to the defeat of Daesh in both Iraq and Syria.[10] Today, most Allies are building offensive cyber capabilities needed to deny adversaries the freedom of maneuver in the cyber domain.

The use of area denial weapon systems in the cyber domain

Anti-Access/Area Denial (A2/AD) weapon systems have traditionally been used by NATO and its member states to prevent an adversary's freedom of maneuver on land, sea or air. In the geographic domains, these capabilities include land mines, missiles (cruise, ballistic, surface to air, anti-ship, etc.), submarines, electronic warfare, and even Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons. In the cyber domain A2/AD is achieved through offensive cyber operations.

Those operations have already been used for the purpose of achieving A2/AD by NATO member states in the cyber domain. This is the case of the US-led Operation Glowing Symphony (OGS), where "the United States Cyber Command reportedly ac-

6 J.M. O'Connor, *International law framework for employing cyber capabilities in military operations memorandum*, US DoD General Counsel, 19 January 2017.

7 D.R. Coats, *Worldwide threat assessment of the US Intelligence community*, ODNI, 2019, p.5.

8 Cybersecurity & Infrastructure Security Agency, *Russian government cyber activity targeting energy and other critical infrastructure sectors, alert (TA18-074A)*, Department of Homeland Security, United States, 2018.

9 M.T. Esper, *Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference*, Department of Defense, United States, 15 February 2020.

10 J. Stoltenberg, *Remarks*, Cyber Defence Pledge Conference, London, 23 May 2019.

quired administrator passwords to [Daesh] websites. The passwords enabled deletion of digital content, including videos used for recruitment, from cyber infrastructure located in at least five countries outside actively hostile areas of Iraq and Syria. Similar digital content reportedly resided on cyber infrastructure in as many as 30 other States. Changing the passwords reportedly locked IS administrators out of the websites".[11] OGS restricted Daesh's freedom of maneuver on networks physically residing in Iraq and Syria (which were controlled by the terrorist group), but also worldwide, where a NATO member state (the US) achieved denial of service effects against Daesh.

OGS disrupted Daesh propaganda through content removal from servers residing in multiple countries and through restricting access to physical infrastructure needed to store digital data. Combined with operational successes against ISIL on the ground, OGS actions resulted in propaganda efforts being significantly reduced on several global social media platforms, including Twitter. One particular offensive cyber operation acted, *ipso facto*, as an A2/AD platform where a NATO member state restricted access to physical networks critical for Daesh recruitment, training, radicalization, fundraising, and command and control.

Integrating offensive cyber capabilities into NATO's mandate for cyber deterrence and defence

Operationalizing warfighting capabilities in the cyber domain, beyond the traditional geographic domains, requires a new way of fighting in the 21st century, challenging the deterrence and defence mandate of the Alliance.

Speaking at the Cyber Defence Pledge Conference in London in May 2019, NATO Secretary General highlighted that for deterrence to have full effect against state and non-state adversaries, NATO and its member states must be ready to use the full range of capabilities at their disposal, to include national offensive cyber capabilities. Deterrence is the act of diminishing an adversary's intent by highlighting the excessive costs for the said adversary if it proceeds with an undesired action. In NATO's case, deterrence is achieved by highlighting to an adversary the excessive costs delivered through military means in the event of an attack against Allies. For deterrence to be successful, the adversary must believe that NATO is ready and willing to impose these excessive costs across all operational domains, to include the cyber domain. This may call for Allies to develop offensive cyber capabilities and integrate them with NATO operations in order to collectively impose a high enough cost to deter adversaries from aggressive behaviour. To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options meant to allow for a gradual increase of pressure in the cyber domain, and then hopefully limiting the scope and intensity of conflict in this domain. NATO Flexible Deterrent Options in the cyber domain could include (as presented in Figure 1):

Offensive cyber operations have already been used for the purpose of achieving A2/AD by NATO member states

- Increasing NATO's readiness posture through cyber education, training and exercises;
- Deploying NATO Cyber Rapid Reaction teams to conduct defensive cyber operations and protecting critical infrastructure of NATO member states and/or that NATO operations rely upon;
- Increasing public awareness of malicious cyber activities and the potential for conflict in the cyber domain;
- Taking steps to gain the support of all NATO member states in response to the cyber threat and in accordance with commitments of the 2016 Cyber Defence Pledge and the 2018 Brussels Summit;
- Triggering Article 4 of the Treaty to enhance information-sharing and mutual assistance in the cyber domain;
- Making official statements addressing violations of international law in the cyber domain;
- Alerting and deploying offensive cyber operations forces;
- Imposing cyber sanctions;[12]
- Conducting offensive cyber operations to achieve A2/AD effects in the cyber domain;
- Triggering Article 5 of the Treaty; and
- Conducting offensive cyber operations in combination with other maneuver forces across all operational domains.

11 S. Watts and T. Richard. "Baseline territorial sovereignty and cyberspace", *Lewis & Clark Law Review*, Vol.22, No.3, 2018, p.772.

12 Cyber sanctions are defined here as "the actual or threatened restriction of digital transactions to affect a behavioural change by a NATO adversary through the introduction of psychological pressure against its political leaders and populace"; see A. Iftimie, "Cyber sanctions: weaponizing the embargo of flagged data in a fragmented internet", *Journal of Information Warfare*, Vol.19, No.1, 2020, p.52.

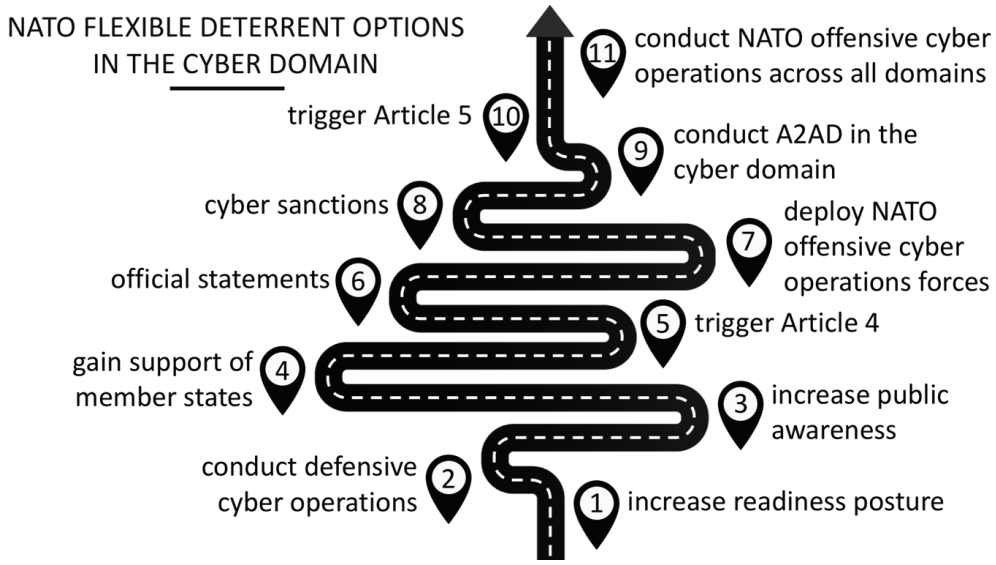

Figure 1: Proposed NATO flexible deterrence options in the cyber domain (author's representation)

NATO Cyber Rapid Reaction teams are already equipped to conduct defensive cyber operations in support of member states if called upon. A mandate of cyber defence and security implies, however, that NATO also starts to engage in active military measures to deny, degrade, disrupt, deceive, or destroy an adversary's offensive cyber capabilities. This requires the development of not only offensive cyber A2/AD capabilities by Allies, but also the restructuring of the NATO command structures, policies, processes (procurement, intelligence, operations, etc.) and engagements needed to integrate them by the Alliance. NATO coordination with both national and regional entities charged with cyber security aspects will, in particular, need to be enhanced. Many agreements already exist in the realm of defensive cyber at national and regional levels (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defence), but political consensus among Allies is missing on whether they should be expanded to incorporate the collective use of offensive cyber A2/AD capabilities.

To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options

Conclusion

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

Successful defence and deterrence in the cyber domain calls, thus, for ready collective offensive cyber A2/AD capabilities that, when integrated with NATO operations, would complement national and/or regional responses to malicious cyber activities. If and when this integration occurs, NATO Flexible Deterrence Options would also need to be agreed upon in order to signal cyber adversaries that Allies will respond with one voice if attacked in the cyber domain. Ultimately, political consensus within the Alliance would still need to be built on the type of needed collective offensive cyber capabilities (such as for A2/AD purposes) and on how to integrate them into NATO's existing operations and missions.

Research Division
Thierry Tardy, PhD, Series Editor
@thierrytardy
NATO Defense College
Via Giorgio Pelosi 1, 00143 Rome – Italy
www.ndc.nato.int

Follow us on Twitter and Facebook
at *https://twitter.com/NDC_Research*
at *https://facebook.com/NDC_Research*
NDC Policy Brief
ISSN 2617-6009