Analysis

NATO's Cyber Deterrence

June 2016

Piret Pernik

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: NATO's Cyber Deterrence
Authors: Piret Pernik
Publication date: June 2016
Category: Analysis

Cover page photo: NATO CCD COE, Estonian Defence Forces (November 2015)

Keywords: Cyber defence, NATO, Deterrence, Cyber domain

ISSN 2228-2076

63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

Introduction

At the Warsaw Summit NATO will recognise cyberspace as an operational domain. According to NATO Secretary General Jens Stoltenberg "treating cyber as an operational domain would enable us to better protect our missions and operations."[1] In this context this policy paper recommends necessary courses of action in order to extend deterrence into this new domain, focusing on education, exercises, training, and evaluation as key aspects for future capability planning. It suggest that NATO should plan and prepare for fulfilling its core tasks — that is, collective defence, crisis management and cooperative security — both in and through the cyber domain.

Deterrence in Cyberspace – from Information to Mission Assurance

Nowadays every geo-political conflict has a cyber component. With more states acquiring military cyber capabilities, and setting up command structures and forces for conducting cyber operations the militarisation of cyberspace is likely to accelerate. According to some estimations 20-30 countries are developing offensive tools for military use. In 2009 and 2010 the US and Israel used the Stuxnet destructive computer virus against Iran's nuclear enrichment facilities, and the US is believed to have developed a virus to attack North Korea's nuclear weapons programme.[2] Adversary countries such as Russia, China, Iran, North Korea possess high-level cyber capabilities. Information warfare and cyberattacks were used as part of Russia's hybrid used tactics in Georgia in 2008 and in Ukraine in 2014. Meanwhile, extremist groups also aspire to obtain offensive cyber capabilities. For example Daesh/ISIS has the capacity to counteract the Allied strategy targeting its fiscal assets, moreover, it possesses the means necessary to begin launching devastating cyber campaigns.[3] In spring this year the US authorized the use of cyber capabilities against the terrorist organisation.[4]

This contested nature of cyberspace was reflected in 2014 in NATO's Wales Summit Declaration: "cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging."[5] According to the NATO's Strategic Concept of 2010 the Alliance "will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations."[6] In Wales the Alliance "affirm[ed] ... that cyber defence is part of NATO's core task of collective defence" and that cyberattacks can lead to the invocation of Article 5.[7] However, NATO's mandate in cyberspace is only defensive, comprising of the protection of its own networks and assisting Allied countries under cyberattack. Hence, the Enhanced Cyber Defence Policy of 2014 focuses on the

[1] Press conference by NATO Secretary General Jens Stoltenberg, 14 June 2016, http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en

[2] http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

[3] ICIT Briefing "The Anatomy of Cyber-Jihad", 29 June 2016, http://icitech.org/wp-content/uploads/2016/06/ICIT-Brief-The-Anatomy-of-Cyber-Jihad1.pdf

[4] http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

[5] Paragraph 72 of the Summit Declaration. http://www.nato.int/cps/ic/natohq/official_texts_112964.htm

[6] Paragraph 19 of the Strategic Concept. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf

[7] Paragraph 72 of the Summit Declaration. http://www.nato.int/cps/ic/natohq/official_texts_112964.htm

protection of communication and information systems (CIS), networks and infrastructure owned by NATO, both during peacetime and mission or operations.[8] By contrast the protection of national assets, including those that are critical for Allied missions and operations, is national responsibility. There are gaps between the levels of protection of Allied countries' networks and infrastructure that NATO missions and operations depend on. NATO has taken steps to mitigate these risks – it has intensified cooperation with industry (NICP), formulated minimum requirements (standards) for national CIS that are either connected or that process NATO information, and pledged to identify dependencies for its critical tasks. NATO has also set up a Cyber Threat Assessment Cell fusing intelligence and information from classified and open sources. These constitute necessary steps in order to ensure information assurance during missions and operations, but they fail to deliver cyber effects in support of missions and operation, i.e. mission assurance.

Even though NATO is a defensive organization, the pledge of collective defence as enshrined in Article 5 is anchored in credible deterrence based on a full spectrum of capabilities in all military domains - air, land, maritime, and cyber. Deterrence is credible only if an adversary fears retaliation. Inflicting destructive damage on an adversary's strategic assets is possible either by offensive cyber or kinetic means. Other countermeasures (political, diplomatic, economic, legislative, etc.) can be used to dissuade an adversary from attacking, but they fall short of credible deterrence. Because not a single network or system is totally secure against cyberattacks or incidents, deterrence by denial alone – that is, a high level of protection – does not seem convincing, while using kinetic attacks as preventive or countermeasures can be considered too escalatory. Thus, without a chance to use offensive cyber capabilities NATO seems to fail to uphold credible deterrence in cyberspace.

Without a chance to use offensive cyber capabilities NATO seems to fail to uphold credible deterrence in cyberspace.

NATO's senior officials underline that the Alliance itself will not develop offensive cyber capabilities. However, many Allied countries possess these tools and have used them in the past, as well as are able to use them in support of NATO operations. Cyber means are highly classified national security information and this renders information sharing among 28 difficult. The haves are reluctant to share information about their capabilities because this exposes their vulnerabilities and gaps. They are not likely to share them with not haves nor delegate authority over them to others. At the same time, due to political sensitivity of cyber weapons and uncertainty concerning the impact of their use, NATO has also refrained from discussing their potential use. However, to ensure mission assurance, the Allied countries should seeks ways to overcome these difficulties and prepare for the possibility of using them in support of NATO missions and operations.

Operationalising the cyber domain

To prepare for treating cyberspace as a military domain, NATO should first update enhanced cyber defence policy to include the potential impact of cyberattacks and incidents on its missions and operations, and the means to ensure mission assurance. It should elaborate common

[8] This responsibility is under the purview of the NATO Communications and Information Agency (NCIA) and NATO Computer Incident Response Capability (NCIRC).

cyber taxonomy and definitions, develop military doctrine for cyber defence, a set of rules of engagement, and operational-level planning guidelines for cyber defence.

Second, Allied countries should address the development of their cyber capabilities in the framework of DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability), the military capability doctrine that provides for assessing and benchmarking maturity levels, identifying capability gaps, and encouraging interoperability.

Third, NATO should work out measures on how NATO commanders can synchronise their activities with the potential use of Allied cyber capabilities in support of missions and operations.

Fourth, NATO's operational commanders require support from cyber defence forces along with a unique operational authority, i.e. cyber command. To support each ongoing military operation, NATO should thus consider establishing a standalone cyber defence force that provides the operation's commander with cyber situational awareness, intelligence, and capabilities. NATO should also invest more in developing operational-level cyber situational awareness.

Finally, it is a truism that education, exercises, training and evaluation (EETE) must be a daily function in cyber defence as threats evolve daily. EETE increase awareness, facilitate trust-building and contribute to better information sharing. Also the integration of cyber aspects into operational-level planning must be drilled regularly by rehearsing cyber threat scenarios, conducting war-gaming, and running simulations.

In order to consolidate NATO's cyber educational and training resources a Cyber Defence Centre under Allied Command Transformation (ACT) should be established. Its mission should be to function as a focal point for cyber defence EETE at the operational level. The Centre would assist ACT in the development of cyber defence doctrine, technologies, modelling and simulation while performing analysis, collecting lessons learned, and feeding them into capability planning. In these efforts the centre could co-operate with the NATO's Joint Analysis and Lessons Learned Centre (JALLC) in Portugal, CIS School in Italy (that will be relocated to Oeiras, Portugal by the end of 2017), and cyber range and NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Estonia. For example, today the CCD COE and CIS School both have courses to prepare officers and civilians from NATO structures and Allied countries for cyber defence. For greater synergy these efforts could be consolidated.

On 10 June this year North-Atlantic Council approved further investments into the NATO cyber range that was established in 2014, raising its technical capability.[9] ACT and Allied Command Operations have been tasked to develop cyber range training requirements.[10] The range can provide a cost-effective hands-on training environment for not only to NATO, but also to its 41+ partners and well as to the EU. NATO has used it since 2013 for its cyber defence exercise Cyber Coalition, also CCD COE's technical level cyber exercise Locked Shields takes place in this facility. In cooperation with the JALLC by identifying, collecting, and sharing lessons learned, the cyber range would contribute to feeding them into capability planning, and improving the implementation of cyber defence into operational planning. Further-

[9] http://www.kmin.ee/en/news/nato-investing-development-estonian-cyber-range

[10] In June 2014 Supreme Allied Commander Transformation approved the Estonian proposal to use the range for NATO. Bruce Jones, "NATO approves new military cyber warfare training centre in Estonia," HIS Jane's 360, 18 June 2014. "SACT and the Estonian Minister of Defence sign an agreement to establish the NATO Cyber Range Capability," http://www.act.nato.int/sact-and-the-estonian-minister-of-defence-sign-an-agreement-to-establish-the-nato-cyber-range-capability; http://www.act.nato.int/sact-and-the-estonian-minister-of-defence-sign-an-agreement-to-establish-the-nato-cyber-range-capability.

more, the range could also serve as a means to test the coordination of the use of cyber capabilities deployed by Allied countries in support of NATO missions and operations. This would contribute to developing arrangements that should be put in place for the use of Allied capabilities in support of NATO missions and operations.

NATO's cyber range could also serve as a means for intensifying partnership with industry and leveraging their technological innovation and R&D activities. In the past NATO has invited industry and academia partners to its cyber defence exercises, and NCIA recently signed agreements with key companies (e.g. Symantec, Cisco, Fortinet) to foster information sharing, enhance situational awareness and increase the protection of NATO's networks and systems.[11] Industry's new solutions and technical platforms could be tested at the cyber range. Finally, the range could share best practices with the Federated Cyber Range of the European Defence Agency that includes cyber ranges for training, research, simulation and testing.[12]

NATO has already intensified cooperation with the EU at the technical level. Since 2011 the NATO and EU computer emergency response teams (NCIRC and CERT-EU) had been cooperating informally, but on 10 February this year their relationship was formalised, enabling the exchange of technical information on cyber threats and sharing of best practices.[13] The EU has also participated as observer in Cyber Coalition exercises.[14]

In conclusion, to maintain credible deterrence in cyberspace, NATO should ensure mission assurance in addition to information assurance. The following steps to strengthen NATO's deterrence in cyberspace are recommended:

To maintain credible deterrence in cyberspace, NATO should ensure mission assurance in addition to information assurance.

1. Update NATO's cyber defence policy, taxonomy and doctrines;
2. Develop a set of rules of engagement and planning guidelines for cyber defence;
3. Develop procedures for the use of Allied cyber capabilities in support of NATO missions and operations;
4. Set up cyber defence force at operational-level and increase investments in operational-level cyber situational awareness;
5. Invest in cyber defence education, exercises, training, and evaluation, including in training and testing capabilities of NATO's cyber range.

[11] http://www.nicp.nato.int/nato-expands-cyber-partnership-with-industry/index.html
[12] http://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/07/13/military-requirements-for-cyber-ranges-agreed
[13] http://www.eeas.europa.eu/statements-eeas/2016/160210_01_en_en.htm
[14] Since 2008, NATO has held an annual cyber defence exercise called Cyber Coalition that tests procedures and coordination in response to cyber attacks (in 2015 more than 750 participants from 33 countries attended the exercise). Beginning in 2012 NATO CCD COE has conducted Locked Shields, an annual technical-level cyber exercise (in 2015 it had 400 participants from 16 countries).

Follow us on:

facebook.com/ICDS.Tallinn

Twitter: @ICDS_Tallinn

linkedin.com/company/3257237

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

Issn 2228-2076