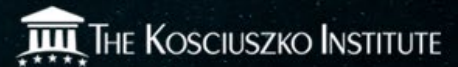


2018 NATO SUMMIT IN CYBER CONTEXT



Nowadays, when NATO faces approximately 5,000 cyber incidents per day, when cyber operations have become one of the main components of hybrid threats used of not only for the purposes of information campaigns or spreading propaganda, when transnational terrorist organisations resort to cyber means and methods to pursue their sinister goals, when destructive potential of cyber tools is not a secret anymore, it comes as no surprise that cyber threats remain high on the agenda of not only NATO, but also the whole international community. Therefore, the Alliance has to remain flexible and agile, become proactive rather than reactive in countering those threats, continue and enhance cooperation with key stakeholders: nations (both members and partners), international organisations, in particular the UN and the EU, but also the OSCE and the Council of Europe (note the Budapest Convention), and the private sector. Outdated or obsolete policies should be amended or revoked without delay, and developments across the whole DOTMLPFI¹ spectrum accelerated to the maximum extent possible.

During the 2014 Wales NATO Summit, Allies recognised that international law (including Law of Armed Conflict) applies in cyberspace, and that the impact of cyberattacks could be as harmful to our societies as a conventional attack and trigger a response under Article 5 of the North Atlantic Treaty. As a result, cyber defence was recognised a part of NATO's core task of collective defence.

What does it mean?

It is now possible to collectively respond to an attack in cyberspace, and it is not different from a conventional attack conducted at sea, in the air or on the land. Evoking Article 5 and NATO's response depends on a political decision – or a judgement call – made by the North Atlantic Council by consensus. What is important, the response does not have to be symmetric or in-kind. NATO's mandate is purely defensive, thus the Alliance does not develop any offensive cyber capabilities, just as it does not develop offensive 'conventional' capabilities. Similarly, the Alliance does not own any equipment or means either (except for the NATO Airborne Early Warning and Control Component). In this regard, it relies on its member states and their armed forces operating in the joint structures. Therefore, it is a national prerogative of the member nations to develop and possess certain defence capabilities, as stated in Article 3 of the North Atlantic Treaty. Those capabilities need to be made available to NATO at its request, as it has always been. This includes providing NATO voluntarily with these national assets in need.

¹ Any combination of Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability.

AN ALLIANCE OF SHARED VALUES AND TRANSATLANTIC UNITY WAS ONE OF THE TOPICS DURING THE 2018 BRUSSELS NATO SUMMIT.

The Summit should endorse the decisions made during the November 2017 Defence Ministerial, particularly the decision to integrate voluntarily contributed national cyber capabilities (including offensive ones) in support of allied operations.

The unit which, among others, will be responsible for operational control over these voluntarily contributed cyber means is the Cyber Operations Centre (CyOC) within Supreme Headquarters Allied Powers Europe (SHAPE) and respective cells in the Joint Force Commands (JFCs). Its creation was approved by Allies during the November 2017 Defence Ministerial. Being 'eyes and ears' of the respective commanders in cyberspace, the CyOC is supposed to enhance situational awareness in cyberspace and help integrate cyber into NATO's planning and operations at all levels. It will not be a cyber command centre as there will not be any supranational command. While the CyOC is to operate within the existing NATO frameworks, its main aim is to equip the Supreme Allied Commander Europe (SACEUR) with all the necessary tools to operate in cyberspace. What still needs to be agreed upon is an overall increase in NATO Command Structure personnel and a greater emphasis on the regional focus of the commands.

Allies should also agree to review NATO's cyber-related policies, including the issue of how NATO should collectively respond to cyberattacks.

The *Cyber as a Domain Implementation Roadmap* identifies 10 Lines of Effort (LoEs). From an operational perspective, the most important ones are the integration of cyber effects and the cyber doctrine development as they are closely related to each other. NATO needs to accelerate the implementation of its Doctrine on Cyberspace Operations to enable cyber operations to be conducted in line with legal, political and military guidelines and principles. Until then, NATO's ability to operate in and through cyberspace, defend in cyberspace equally efficiently as on the land, in the air or at sea, while at the same time acting within the boundaries of international law and in line with the principles of responsible behaviour, will remain limited.

At the 2014 Wales NATO Summit, Allies reaffirmed their commitment to spend a minimum of two percent of each Ally's GDP on defence.

Moreover, the Cyber Defence Pledge from the 2016 Warsaw NATO Summit commits Allies to allocate adequate resources nationally to strengthen their cyber defence capabilities, even if there is no specified minimum amount.

FAIRER BURDEN-SHARING WAS ONE OF THE MOST IMPORTANT TOPICS DURING THE BRUSSELS NATO SUMMIT.

And it will not leave the table as long as the U.S. continues to contribute the most to NATO's total military spending. According to estimates from 2017, only six members fulfilled the two percent requirement², with only eight countries estimated to do so in 2018. However, even with eight NATO Allies hitting the target, it leaves 21 behind. The situation will become more dramatic for Allies in the European Union after Brexit as the contributions of non-EU NATO countries (the U.S., the UK, Turkey, Canada and Norway) will account for staggering 80 percent or so of the total budget.

During the Summit, the progress in defence expenditures that has been achieved in recent years should be acknowledged; therefore, it should be also highlighted that this has not yet occurred across the whole of the Alliance.

Defence expenditures shall be further increased, and national plans are needed to achieve commonly agreed goals as part of this commitment, including cyber goals. There is a need for European leaders who show political will and

² According to the UK Defence Expenditure report from 22 February 2018.

leadership to convince their electorates that Europe must do more for the military, so that credibility of Europe's defences is regained.

During the 2016 NATO Summit in Warsaw, Allies pledged to strengthen and enhance the cyber defences of national networks and infrastructures as a matter of priority.


What does it mean?

RESILIENCE WAS THE BIGGEST PRIORITY FOR ALLIES DURING THE 2018 BRUSSELS NATO SUMMIT.

Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term development, the Cyber Defence Pledge will reinforce the cyber defence and overall resilience of the Alliance. As NATO depends on national capabilities in nearly every area, its ability to operate in the cyber domain also hinges upon its success to set more ambitious capability targets for its member states and to encourage them to plug the identified gaps. By inducing Allies to perform more regular assessments of their levels of preparedness, the Cyber Defence Pledge should make this effort easier in the future.

STRENGTHENING DETERRENCE AND DEFENCE WAS DISCUSSED DURING THE 2018 BRUSSELS NATO SUMMIT.

National development concerning the Cyber Defence Pledge engagements will be assessed for the first time with regard to the set criteria.



Allies have carried out self-assessments of their cyber defence hygiene by reporting on seven capability areas: strategy, organisation, processes and procedures, threat intelligence, partnerships, capabilities, and investments. They were supposed to benchmark these assessments according to four levels ranging from advanced to a relative beginner. These assessments will allow NATO staff to develop more precise and relevant metrics, to form a more reliable common baseline of overall NATO capabilities, as well as to identify gaps and prioritise requirements. On this basis, the well-known NATO Defence Planning process, which has already incorporated a set of basic cyber capability targets for each NATO member state, will be able to suggest more ambitious targets that are better adapted to the needs of individual states in the future. The peer pressure that greater transparency should create will incentivise Allies to meet their assigned targets and to stimulate bilateral assistance. The process should also help identify best practices. The results will be published in a report available only to the heads and the governments of the member states.

Although the details will not be available to the public but shared only within and among the Summit participants, it is safe to assume that Poland will be among the leaders in the delivery of the Pledge. There is a number of arguments behind this assumption.

Firstly, Poland has been one of the pace-setters in the cyber defence area, at least in the European part of the Alliance, which was demonstrated e.g. in the course of the preparations to the 2016 Warsaw NATO Summit during which Poland actively lobbied for recognising cyberspace as an operational domain. Secondly, Poland has been proactive in the cyber defence area over the last decade. Recent decisions made by the Polish government in general and the Ministry of National Defence in particular regarding the consolidation of Polish military cyber capabilities under the auspices of the National Cryptology Centre, the creation of cyber units within the Polish Armed Forces, or the pursuit of development of both defensive and offensive military cyber capabilities confirm Poland's commitment to strengthening cyber resilience and cyber defence. Thirdly, the decision to build the state's cybersecurity system with the Ministry of National Defence in charge, despite being controversial for many reasons, clearly indicates that the Polish government recognises the importance of the military in the overall cybersecurity or cyber defence system.

Also, the goals established by the resolution of the Polish government about 'Detailed directions for rebuilding and modernization of the Armed Forces for years 2017-2026' from June 2018 are in line with the recommendations of the *Strategic Defence Review (Strategiczny Przegląd Obronny)* and are a sign of positive change. They are also a proof of increased awareness in this area. The resolution forms the basis for further work to be done in the defence department, such as the establishment of the Plan of Technical Modernisation for the years 2017-2026. However, even though there is a legal requirement that says the spending on defence should reach 2.5 percent of the GDP until 2030, it still may be insufficient to cover the modernization expenditure required for the Polish army in the coming years.

There are some leading countries in the area of cyber defence, such as the U.S. or Estonia, but none of the Allies is fully ready to face cyberattacks, as none of them is fully resilient. Some of them handle them better than others, but still the challenges are the same for all of them. However, the question is not exactly about the readiness – it is more about the mindset and the situational awareness: there is nothing like being fully ready, there is always a gap that needs to be filled, even in the case of the best performing actors.

NATO's relations with the European Union have been considered as 'Strategic Partnership' since the 2010 Summit in Lisbon. Since the 2016 Summit in Warsaw, the EU has significantly increased its profile and activities in the defence field, predominantly by launching the Permanent Structured Cooperation.

Just before the 2018 Brussels NATO Summit, Secretary General Jens Stoltenberg signed a new Joint Declaration with European Council President Donald Tusk and European Commission President Jean-Claude Juncker, setting out a shared vision of how NATO-EU cooperation can help address most pressing security challenges, including hybrid and cyber threats.

The Summit was an opportunity to enhance further the relationship between NATO and the European Union. The NATO-EU Joint Declaration signed during the 2016 Warsaw NATO Summit highlighted hybrid threats and cyber defence as key areas for cooperation between the two organisations.

The Summit should provide an opportunity to review progress in cooperative projects, as their implementation, not only further declarations, must now be at the heart of the relationship.

There is a Technical Arrangement on cyber defence between NATO Computer Emergency Response Teams and CERT-EU which enables the exchange of information in real time. Both organisations are also members of the Malware Information Sharing Platform that gives them access to each other's databases. Moreover, regular meetings are held during which NATO and the EU representatives share best practices. The results are practical and pragmatic. There is an idea to expand this cooperation within the Technical Agreement.

Both organisations strengthen cooperation in cyber exercises through reciprocal staff participation in respective exercises, including Cyber Coalition and Cyber Europe in particular. Last year, the EU took part in the Cyber Coalition exercises for the first time. Crisis Management Exercises are more of a strategic type of exercises comprising cyber as part of a global defence framework. They are focused on cyber matters in a hybrid environment. In general, this is a good example of strategic and operational cooperation between the two organisations.

NATO Cooperative Cyber Defence Centre of Excellence in Tallinn would probably be the best institution to develop a common NATO-EU framework on how to respond to threats and activities in the cyber sphere.

NATO has reached a turning point when it comes to ensuring its security and the 2018 Brussels NATO Summit was an important opportunity to make the Alliance better equipped to handle emerging new challenges. The Summit lasted two days, but will certainly impact the years ahead.

AUTHORS:

Marta Przywała is Research Fellow in the Kosciuszko Institute and CYBERSEC Project Manager. Her main areas of expertise are cybersecurity, and international security and defence. She graduated in French language and literature at the Jagiellonian University in Krakow. She holds double MA degree from the Centre for European Studies of the JU and Institut d'études politiques of the University of Strasbourg. She was granted the French government fellowship.

CDR Wiesław Goździewicz is Legal Adviser at NATO Joint Force Training Centre in Bydgoszcz, as well as Expert of the Kosciuszko Institute. He provides legal advice and training on the practicalities of the application of international humanitarian law and legal aspects of military operations. He served at the Public International Law Division of the Legal Department of the Ministry of National Defence. Commander Goździewicz (Polish Navy) joined the Armed Forces as a junior legal officer, at the 43rd Naval Airbase in Gdynia. He is a graduate of the Faculty of Law and Administration of the University of Gdańsk.



The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000.

The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.

The Kosciuszko Institute organizes the European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.

Office: Wilhelma Feldmana 4/9-10, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl,
e-mail: instytut@ik.org.pl

More on the CYBERSEC European Cybersecurity Forum: <http://cybersecforum.eu/>

More on the European Cybersecurity Journal: <http://cybersecforum.eu/en/about-ecj/>