Protecting European networks: What can NATO do?

by Sophia Besch

31 October 2018

With the 'cyber defence pledge' NATO is trying to get its allies to do more to protect their networks. The alliance should lead by example.

Unprotected computer networks are a security threat. Adversaries can obtain military secrets by breaking into the information and communications systems of a military force, business or nation state. They can also target and interfere with civilian 'critical' networks essential for everyday life, such as nuclear reactors, telecommunication companies, power plants and water supply facilities. NATO has had to adapt to this new security threat. This insight evaluates the progress the alliance has made so far as well as the challenges it still faces in the areas of resources, procurement, personnel, training and information sharing.

NATO has to wrestle with a range of challenges under the broad headline of cyber defence. Most recently the alliance has been tackling the question of how to integrate 'cyber' into NATO planning, training, exercises and operations. It has officially recognized cyber space as an operational domain. But as in the conventional domains of air, sea, land and space, NATO does not own any offensive capabilities itself; it relies on its allies to offer their cyber capabilities to support NATO operations. The alliance's primary, and most urgent cyber task is the protection of the communications systems and networks owned and operated by NATO.

In recent years NATO has also started working on helping allies help themselves. So-called NATO Cyber Rapid Reaction teams are on standby to assist NATO nations suffering a cyber attack. The alliance also offers training opportunities, tries to make information sharing between member-states easier, and pressures allies to do more at home. But NATO has no legal enforcement mechanisms, and persuading the allies to strengthen their cyber defences is a challenge. In defence spending, a more traditional field of NATO responsibility, the alliance has a high-profile instrument at its disposal to exert pressure on allies: the two per cent pledge. NATO has decided to take an analogous approach to its cyber work.

The 'cyber defence pledge' was conceived in 2016 as a political instrument to expand NATO's cyber mandate. It makes NATO responsible not just for protecting the alliance's networks but also for setting

best practices and standards and raising awareness in capitals. The pledge commits allies to allocate adequate resources nationally; engage in the exchange of best practices; share information and assessments; enhance skills and awareness among all defence stakeholders at national level; and organise cyber education, training and exercises to build trust and knowledge across the alliance. In practice NATO monitors the implementation of the pledge through surveys, which allies fill out in bilateral meetings between HQ and whichever national authority is responsible for cyber issues. Here NATO has had to adapt, since these national authorities are often not a traditional NATO partner such as a defence or foreign ministry, but another agency, like the Federal Office for Information Security in Germany or the National Cyber Security Agency in France.

NATO allies have now begun to allocate more resources to the protection of national networks. It is difficult to tell how much of that progress is linked to the cyber pledge: repeated cyber attacks on NATO allies in recent years have given them good reason to invest voluntarily. However, like the two per cent defence spending pledge, the cyber pledge can be useful in giving added political legitimacy to those warning of the need for urgent action and pushing for increased cyber spending.

Unlike the two per cent pledge, however, it can be hard to tell how much cyber spending is enough. Computer hardware and software are cheap compared to conventional defence kit such as fighter jets, even if the cost of training humans for cyber tasks is high. One problem is that there is no simple formula for how much cyber defence is required. NATO has always justified its defence equipment requirements by asking allies to match the armament efforts of hostile countries, in particular Russia. It is difficult to quantify cyber requirements in the same way.

Instead the cyber pledge focuses on the effects of investment, such as whether a member-state is able to monitor a network 24/7, or to detect and trace attacks. A simple comparison of cyber strength between NATO and Russia, North Korea or China is difficult. But many point to the strength of Western countries in innovative technologies as a considerable advantage. Still, NATO struggles to reap the fruits of the innovative businesses located in its member-states. Its lengthy and often overly bureaucratic procurement process restricts NATO's ability to access the newest cyber defence technologies. In a field where technology is moving very fast, NATO will forever lag behind if it cannot reform the way it procures cyber capabilities.

One of NATO's 'smart defence' projects could offer a solution to the alliance's cyber procurement troubles. The smart defence initiative enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone, and to free up resources for developing other capabilities. The Multinational Cyber Defence Capability Development (MNCD2) smart defence project addresses one of the problems vexing NATO's procurement process: over-specification. Over-specifying cyber requirements is particularly problematic, as military personnel often do not fully understand the technologies they are asking for and the pace of technological change is so rapid that the delays and disruptions caused by poor requirement definitions are even less tolerable than for conventional weapons. In MNCD2, participating militaries outline a set of potential scenarios for how the necessary capability would be used and then leave it to innovative industry suppliers to work out how to best deliver the desired operational effects: rather than asking for a specific type of anti-virus programme for example, which could be outdated by the time the supplier delivers, militaries would instead ask for a programme that protects their networks from relevant threats.

When it comes to protecting their networks, another major challenge for NATO and its member-states is finding, training and retaining the right people. The real shortcomings identified in many bilateral cyber pledge meetings between NATO Headquarters and member states are often the training and education of domestic personnel. Through the cyber pledge meetings, NATO is spreading best practice among allies for recruiting and retaining experts, particularly cyber forensics specialists. But the demand for these skills is far higher than the supply: if modern technology and competitive salaries are not available in ministries and international organisations, the best talent will probably go into the private sector.

At the same time, the cyber pledge will not work unless the private sector is also involved: NATO should embrace its role not just as a platform where allies can share information, but also as a forum for exchanges with industry. Businesses will often have experienced similar or worse attacks on their networks than NATO, and member-states and can share lessons learnt. NATO has established a platform to share information with industry, but the database is only being used for unclassified technical characteristics of malware for the time being, and thus is limited in its usefulness for users. Allies remain unwilling to grant others – industry or other governments – insights into details gathered on past cyber attacks and potential threats they have identified. Most crucially, they do not want to share information about their own vulnerabilities and preparedness. So NATO's role is limited to helping the weakest governments to improve their resilience (often by connecting them with better-resourced ones), increasing mutual trust between states and the private sector, and thus making countries feel more comfortable about gradually being more open.

The alliance also has a clear security interest in fostering civil-military and public-private co-operation in the field of network protection. Not all critical infrastructure networks are under military or government control. But at the moment, if, for example, a power plant in a NATO member-state were suddenly to shut down, NATO Headquarters would probably not be the first number a company called, even though the security and defence implications of a compromised electricity grid could be severe. In spite of their importance, civilian networks are currently left to individual NATO allies to look after. An attack on civilian infrastructure networks could be both economically damaging and a defence threat: for example, if an attacker hacked the German rail network at a time of tension, they could prevent NATO reinforcements moving forward, and simultaneously cripple the German economy. This is an obvious area for NATO-EU co-operation.

NATO and the EU have stepped up their co-operation efforts in a number of areas in recent years, with cyber security high on the list. In a parallel effort to NATO's cyber pledge, the EU in July 2016 adopted a directive on the security of network and information systems. The directive sets minimum standards, but could have important effects, requiring operators of critical infrastructure to report significant attacks on their networks to specialised teams set up by member-states. Implementation has been slow so far: only 11 EU countries had transposed the directive into national law by the May 2018 deadline. But the EU, in contrast to NATO, is a legal regulator with enforcement mechanisms at its disposal. And it is intensifying its activities in the field of cyber security, on standard setting and certification, for example. The EU's most recent efforts to strengthen Europe's defence industrial base could have implications for European cyber capabilities as well: the Commission wants to invest money from the new European defence fund in cyber research and development. Two cyber projects have been launched as part of the EU's new Permanent Structured Co-operation (PESCO) framework: an information-sharing platform for cyber incidents and cyber rapid response teams.

Both NATO and the EU also profit from exchanging best practices in the areas of education, training and exercises. NATO has for example shared its complete education and individual training syllabus, featuring NATO's cyber defence courses, with EU staff. For the first time, EU cyber defence staff took part as full participants in NATO's Cyber Coalition exercise held at the end of 2017. And in April 2018, EU staff participated in the NATO Locked Shields exercise, organised by the NATO Cyber Center of Excellence in Estonia. Both NATO and the EU need to start thinking in a joined up way about the cyber threats they face. But the exchange with the EU remains slow and formal, limited to non-classified information.

Europeans can benefit from sharing information when it comes to protecting their networks. But while NATO can offer useful tools and a secure environment, it always relies on national players to provide input on the cyber attacks they have experienced and the tools they are developing to defend against future incidents, not least because once a cyber measure has been deployed and its effect revealed, its potency is lost and it can often never be used again.

NATO should lead by example: it should reform its acquisition processes to fit the development cycles of cyber technology, make sure that personnel are trained to see the cyber security dimension of their everyday work, seek out co-operation with industry, and improve its co-operation with the EU through better information-sharing mechanisms and more joint cyber exercises. But to get its allies to increase their efforts domestically and to learn from each other, NATO still relies primarily on peer pressure. The hope is that the cyber pledge will be more persuasive than its defence spending equivalent.

Sophia Besch is a reserch fellow at the Centre for European Reform.