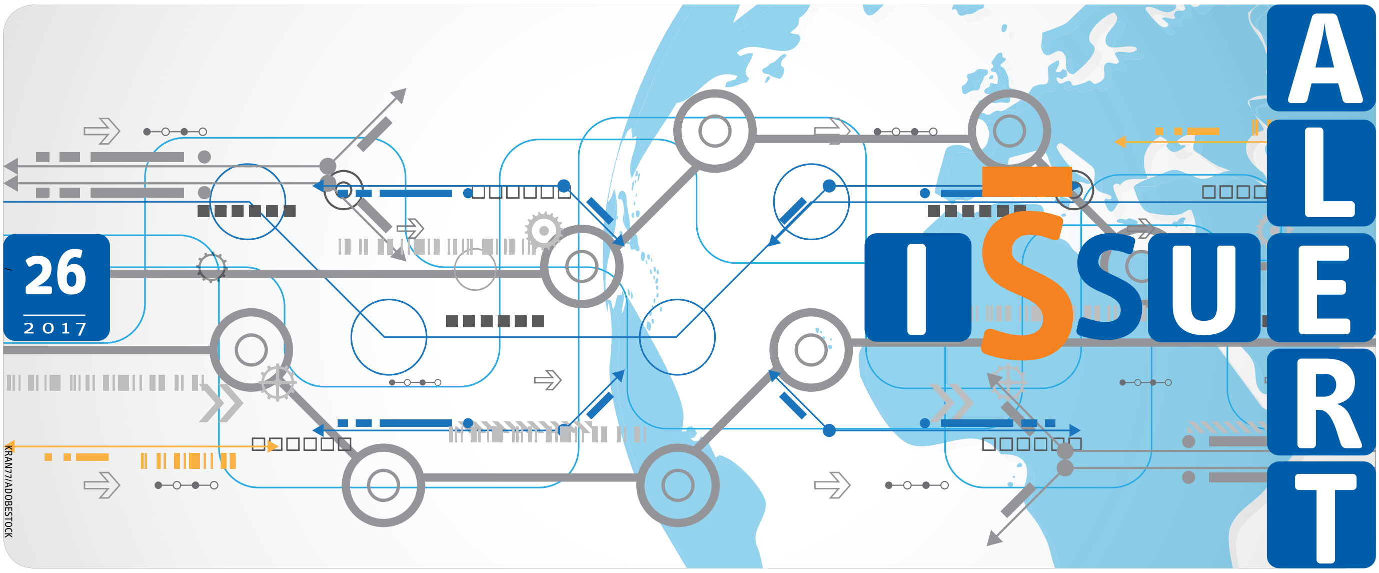

ISSUE ALERT
26
2017
KRAN77/ADOBESTOCK

Building capacities for cyber defence

by Patryk Pawlak

With Ukraine's national bank, state power company and largest airport having all been targeted by malicious cyber activities, there is little doubt about the link between the security of critical infrastructure and human development. Such attacks are even more worrying when they form an element of a hybrid conflict between states, increasing the risk of escalation. And yet, strengthening the security capacities of state actors in the cyber domain is still an unorthodox issue on the development agenda. This is despite the explicit inclusion in the UN's 2030 Agenda for sustainable development of building resilient infrastructure (Goal 9) and the promotion of peaceful and inclusive societies for sustainable development (Goal 16). In this sense, the decision by the OECD Development Assistance Committee (DAC) not to include contributions to the NATO Cyber Defence Trust Fund in a recently updated Official Development Assistance (ODA) Casebook on Conflict, Peace and Security Activities represents a missed opportunity to clarify the link between defence and development in the case of cyber defence capacity building.

To do or to DAC: that is the question

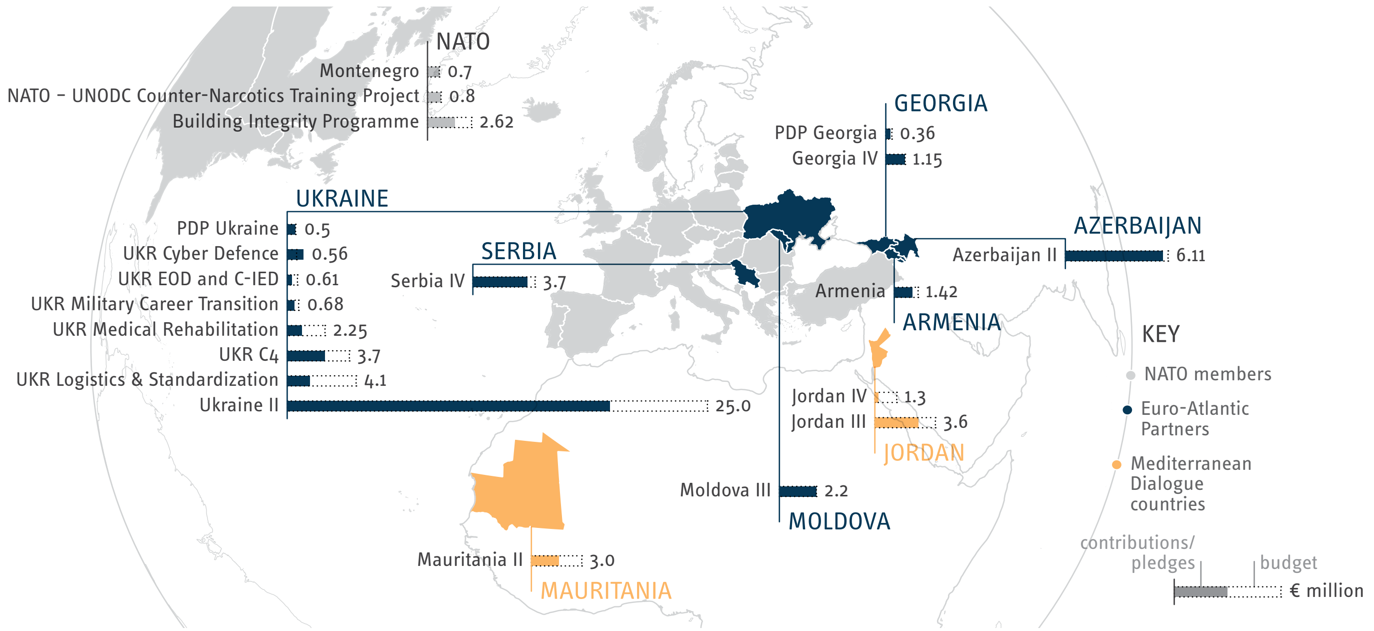
Taking into account the Partnership Goals agreed within NATO's 2012 Partnership for Peace Planning and Review Process (PARP), a Trust Fund on Cyber Defence for Ukraine was set up with the aim of providing Kiev 'with the necessary support to develop its strictly defensive, CSIRT-type technical capabilities'. Declared operational in December 2014, the Trust Fund has attracted nearly €1 million in funding, plus in-kind contributions offered by Estonia and the US. Led by Romania and with contributions from seven other countries, the Trust Fund financed the creation of two Incident Management Centres to monitor cyber security events, laboratories to investigate cyber security incidents, and training. The second phase of the implementation of the Trust Fund was announced in the joint statement of the NATO-Ukraine Commission in July 2017. Although the Trust Fund was initially part of the reflection on ODA eligibility of activities involving military actors, it was no longer included in the final casebook endorsed by the DAC High Level Communiqué of 31 October 2017.

The debate about the link between security and development is not a new. But as the risks and the security environment evolve, traditional development actors no longer hold the monopoly or are well-equipped to provide the support required. Consequently, other actors – including the military and law enforcement agencies – are forced to step in. At the same time, the development business is not what it used to be: security actors are increasingly competing for resources with programmes focused on poverty eradication or gender equality. Activities like training on the protection of human rights, building capacity to combat and prevent radicalisation, terrorism and money laundering, or cybersecurity-related initiatives all create ambiguity for ODA reporting.

The decision by the OECD DAC in February 2016 to update and clarify the ODA reporting directives on peace and security created an expectation in the

NATO Trust Funds

in € million, as of Oct 2017



Data: NATO

security community that a less ideological approach was possible. Given that the financing of military equipment or services or activities combatting terrorism are in general excluded from ODA reporting, the inclusion of cyberdefence-related projects as 'DAC-able' in the revised ODA Casebook has been described as a potential 'earthquake' in the development community. In that sense, the failure to provide clear guidance on the 'DAC-ability' of cybersecurity assistance and capacity building for cyber defence only prolongs the uncertainty related to such spending and might inhibit future initiatives in this domain.

Cyber's defence-development nexus

The key issue in the debate is the dual use nature of cyber tools: the difficulty in constraining the potential misuse of equipment or skills delivered for purely defensive purposes weighs heavily on decisions to provide assistance. However, it is not impossible to compile a catalogue of institutional, legal or human capabilities where the lines between offensive-defensive and civilian-military actions are less problematic. In fact, any large-scale cyber attack is very likely to demand a comprehensive and integrated civil-military approach. Therefore, the establishment of the Incident Management Centres or providing training in digital forensics in a given country would be welcomed by cybersecurity experts as a step towards strengthening the resilience of society as a whole. At the same time, the political risks associated with offensive cyber operations are mitigated by the fact that such operations remain the responsibility of individual states which are subject to existing international law, including the UN Charter.

In addition, in the longer term cyber defence capacity building initiatives contribute to reducing 'cyber anxieties', the risks of miscalculation, and eventually may minimise the risk of conflict. As states improve their understanding of risks in the cyber domain and build resilience to address their vulnerabilities, they strengthen their own 'cyber immunity system' and are less likely to overreact. A country with decent situational awareness, an understanding of the events at hand, and a broad range of mitigation and response tools is less likely to consider a cyber incident as an armed attack. In other words, building cyber (defence) capacities strengthens state and societal resilience, which in turn increases the threshold of armed conflict. This is important because neither NATO nor the EU have set a threshold for an armed conflict in the cyber realm, leaving this decision to individual member states.

Against this background, it is important for both the EU and NATO to remain action-oriented in order to protect their economies, political institutions, and fundamental freedoms. The adoption of the joint EU-NATO Declaration in July 2016 has paved the way for intensifying cooperation in countering hybrid threats, cybersecurity and defence, as well as building the defence and security capacities of partners in the east and south. The next report on EU-NATO cooperation, to be submitted to the respective Councils in December 2017, provides an opportunity to consider the way forward, including closer coordination on capacity building for cyber defence.

Patryk Pawlak is the Brussels Executive Officer and is responsible for cyber-related issues at the EUISS.

© EU Institute for Security Studies | QN-AL-17-026-2A-N | ISBN 978-92-9198-533-3 | ISSN 2315-1129 | doi:10.2815/379783