Latvian Presidency of the Council of the European Union
EU2015.LV

Ministry of Defence
Republic of Latvia

Federal Ministry of Defence

‘Cyber Defence in Europe’ Conference

25 - 26 March 2015, Berlin / Germany

Conference Report

Upon invitation by the Latvian Presidency of the Council of the European Union, supported by the German Federal Ministry of Defence, more than 100 European leading experts on cyber defence met at the conference ‘Cyber Defence in Europe’ in Berlin on 25-26 March 2015.

In her opening address, the German State Secretary Dr Katrin Suder introduced the subject by highlighting the changing international security environment and the increasing importance of cyber hybrid warfare scenarios. She highlighted the necessity to adapt capabilities, i.e. means, structures, and equipment, to meet future challenges and called for the involvement of parliaments, media, and civil societies in such process. In terms of future action, she called cyber a ‘team sport’ which includes various national and international players, and for sufficient awareness at the highest level.

The Latvian Secretary of State Jānis Sārts described the challenges of the digital age in his key note address. He stressed the vulnerability of societies due to their heavy reliance on cyber infrastructure. However, he questioned the way of looking at cyber as a merely technical issue. To overcome this shortcoming, he stipulated strategic leadership in this area. The threat would have to be seen in a wider context, including international crises, economic growth, or job security. Eventually, he reflected on possible solutions, for instance two Latvian projects that are currently ongoing: a national cyber defence force with voluntary support from civilians, and a training project for children.

Panel I: Implications of the EU’s Cyber Defence Policy Framework

During panel I the main features of the ‘EU Cyber Defence Policy Framework’ were looked at from an EEAS perspective, followed by an academic insight, and by an intervention from a national (Dutch) view. The panellists focused on its implications for the EU/CSDP and Member States. It was shown what the policy framework has achieved in terms of strengthening cyber defence in Europe so far, how the policy framework will be implemented, what the EU and what the Member States need to do, and what still remains to be agreed upon in the future in order to further strengthen cyber defence in Europe. Some interfaces, e.g. between Member States and the EU, civil and military, the political and the technical level, defensive and offensive capabilities, and between organisations such as EU and NATO were identified. Inconsistencies came up during the discussion as well: were the right priorities chosen? Does the EU have the appropriate capabilities? Are Member States willing to share knowledge, standards and intelligence in the defence domain? The Netherlands presented their way of developing from a level of awareness to a level of ‘being skilled’ in cyber

matters, and identified cooperation as a key success factor for the implementation of their cyber strategy. Some innovative approaches to attract the best cyber talents to work for governments and defence were added, including a proposal for a 'cyber Erasmus'.

Panel II: The EU's Mutual Defence and Solidarity Clause in the Cyber Context

The speakers of panel II discussed the EU's mutual defence and solidarity clauses. A legal presentation introduced the theoretical and legal features of the two clauses, and described their applicability in the course of major 'cyber-attacks'. The European Parliament representative depicted the mechanisms underpinning the clauses, the administrative and political processes in place in case of major cyber-attacks, as well as potential shortcomings in the system with regard to cyber threats to be solved. Finally, the topic was approached from a national viewpoint (Finland), including what the obligation to mutual defence and the concept of solidarity could entail for the country in case of major 'cyber-attacks'. In the discussion, the question of modular defence was raised by the moderator, considering that a unification of standards and interoperability also leads to much higher vulnerability of systems. Since cyber defence will always be one step ahead of the defence, deterrence was identified as a major strategic surplus, although only valid in the context of state actors, but meaningless as regards non-state actors. Eventually, the applicability of the clauses casts a doubt on the EU's political will to not only declare but act as a defence organisation.

Panel III: Cyber Defence in EU Military Operations

Panel III presented the current state of endeavours to ensure and to strengthen cyber defence in EU-led military operations. The challenges and obstacles the EU and the Member States (especially those operating an EU OHQ) face, different policy actions undertaken currently by the European External Action Service and EU Member States, and diverse projects within the European Defence Agency were depicted. The description of the measures undertaken to strengthen cyber defence in EU-led military operations was followed by a presentation from a practical view, namely by EUFOR RCA. The EU's dependence on Member States' military assets was identified as an obstacle, as well as the non-permanent, ad-hoc arrangements and the dependence on civilian actors. Also, there is a need to refocus the military dimension on cyber defence (as opposed to IT-security). Personnel, process and procedures, as much as technology determine the success, but have to be de-conflicted with other mission considerations. As regards personnel, the question of how to attract the best talents remained an issue of concern.

Panel IV: Civil-Military Cooperation in Cyber-Defence

Panel IV discussed possibilities for civil-military cooperation in cyber defence. First, the synergies which can be achieved between the civilian and the defence cyber security research and markets and the endeavours undertaken in this regard by the European Commission were outlined. This was followed by a presentation on the Cyber Defence Unit of the Latvian National Guard, an entity linking the constitutional mandate of the armed forces to (cyber)defence in case of major 'cyber-attacks' that amount to an 'armed attack' and the potential for cyber defence actions on a bit for bit basis that are existing within the civil society and industry. Last but not least, a practical example of civil-military cooperation between the EU and a private company was presented. *Inter alia*, the endeavours of the company, tasked to provide secure, reliable and efficient communication platforms within Europe, the obstacles (different cultures, different security approaches,

political sensitivities, different legal systems), the different requirements for various information (sharing) systems were described. The discussion centred on best practice for cyber defence units, including the 'team sport' aspect, i.e. building a pool of competent people who are not necessarily military but work in government, KRITIS of business, but are ready to lend support in case of crises. As to business, one dilemma was picked out as a central theme: more security causes more costs and time which both reduce profit.

Conclusions

As regards the implications of the Cyber Defence Policy Framework, cooperation (at political, technical, legal level) amongst Members States was identified as key to make it a success. Impediments for cooperation consist *inter alia* of diverging industrial interests, a lack of trust, and last but not least a presumed reluctance from Member States to transfer sovereignty – which could be rooted in a lack of political will to do so, despite the major role the EU could play in fostering coordination, generate cooperation, and thus pave the way towards integration. The discussions around the solidarity clause identified unanimous decision-making procedures as counter-productive to progress. Whilst CSDP missions are the reality check for CSDP and its capabilities, the challenges to be solved for futures missions remain to be looked at in detail. In the field of civil-military cooperation, the research programmes by the European Commission and their potential for CSDP as well as the cooperation with EDA need to be further explored and strengthened.

Action Points

Speakers, panellists and participants stressed the increasing importance of cyber defence, also in the political arena. The Latvian Presidency therefore encourages Member States to address the issue at national level, but will also continue promoting cyber defence at EU level in the respective fora. With a view to produce tangible results, the following action points will be proposed:

- Encourage cross-departmental, cross-agency as well as bilateral and multilateral cyber cooperation to bring live to the idea of cyber as a 'team sport'.
- Exchange best practice, training and awareness aspects amongst Member States and other international organisations.
- Continue the implantation of the EU Cyber Defence Roadmap with increased efforts.
- Consider further aspects of cyber defence, e.g. cybercrime, cyber terrorism, when establishing future projects.
- Develop cooperation with business, academia and young people to create a sustainable network of competent experts, also with a view to reach out to the public more successfully.
- Aim at responsible, informed, and skilled users in the European Union as the ultimate cyber defenders on a day-to-day basis.
- Ensure that the issue of cyber and cyber defence receives adequate attention in both the upcoming Council and European Council conclusions as well as a revised European Security Strategy.