"We need to collaborate to create our own joint capabilities"


© Cybernetica

Europe's security, and that of its Member States, will rely more and more on its ability to be up to speed with the most innovative and disruptive cyber technologies to counter growing threats from cyberspace. Lagging behind in this domain compared to the US or China, Europe must urgently overcome its national fragmentation, make a quantum leap in cyber defence cooperation and create the right conditions for research and industry to compete, says **Oliver Väärtnõu**, the CEO of Cybernetica AS, an Estonian cyber company, in the following exclusive interview.

Some experts predict the next war will happen in cyberspace. With the technological insight you have, is this a real threat?

I guess it all depends on the definition of war, but a cyber conflict is definitely a threat one has to seriously consider and that has already materialised in various countries, e.g. in Ukraine, Estonia etc. As countries become more and more digital and reliant on technologies, it becomes a lucrative attack vector to our adversaries. For example - why consider the use of kinetic force to attack a powerplant if you can instead organise a cyberattack against it that achieves the same impact when it stalls or interferes with the turbines? Or alternatively, take down a banking, payment system in a country, where the share of cash payments is less than 20%? Or take over control of self-driving cars and direct them against their users, or pedestrians with possible lethal effects? One can definitely create a lot of havoc and uncertainty only by using cyber as the domain of operation. Moreover, bear in mind that preparing physical attacks often requires much more resources and is so to speak 'louder' than achieving the same goals via the digital environment.

How well - or badly - are Europe's Armed Forces prepared for such a scenario?

I think one has to make a clear distinction between, on the one hand, how well the military is prepared to protect itself against cyberattacks; and, on the other hand, how well the military is equipped to protect society against such attacks. Currently the main focus is dedicated to building up capabilities to protect itself and also, to some extent, to create offensive capabilities. The wider protection of society, however, is not actually under the control of the Armed Forces. In peacetime, civil law enforcement organisations are and should be in charge of the cyber domain, but they need to work closely with the military and share all necessary information with them, as they will have to act in a real conflict situation. In this context, a key aspect is to assess whether an incident is so severe that it is worth declaring a state of war against another country or if it is just a hacking incident that doesn't need escalation. Furthermore, one has also to bear in mind that in the digital space, it is much harder to attribute an attack to an adversary than in conventional warfare. →

How competitive is Europe's cyber security & defence industry, compared to other players in the world?

By looking at the big picture, one can say that Europe so to speak 'discovered' cybersecurity as a domain only when the previous European Commission, headed by Mr. Juncker, took office. Since then it has been one of the priorities of the Commission and also an important topic within the Member States. Of course, cyber incidents during elections, e.g. in Germany and France, have also increased its political importance. Nevertheless, it is fair to say that Europe does not have as strong a cybersecurity industry or companies than the US or Israel or even China. Looking at the investment levels and ecosystems developed via industrial policies, we have a long way to go to compete. Though, the signs today are promising – the EU is directing more funding, initiating discussions, and creating an EU Cybersecurity Competence Centre network to develop expertise in the field. We have good scientific and research potential in Europe, but it does not predominantly express itself in companies but is rather concentrated in research institutes and government institutions.

What are the main stumbling blocks for improving cyber defence and security in Europe? What is missing, what needs to change?

What the EU lacks most, compared to its biggest competitors, namely China and USA, is unity. Today we are in a situation where 27 Member States look at cybersecurity as something that is critical to their national capability and, therefore, they are keeping their markets closed and their contracts local. Although we boast that we have one of the largest internal markets in the world, it is not really the case for the cyber domain. We hope that the initiatives taken by the Commission, like the European Certification Scheme, will provide means to overcome these issues, but time will tell. Also, we must consider how the European industrial complex works and what is the right balance between public and private sectors? In terms of investments, the situation has improved significantly over the years both from a research investment perspective, as well as regarding access to venture capital. However, comparing ourselves to the US and China, it is clear that we still need more emphasis on funding cybersecurity. For example, Europe does not have a dedicated venture capital industry for cybersecurity companies, like the US does. Another issue that I would like to raise and that requires our attention, is cross-border and national information sharing. If we want to create knowledge in this domain, we need to build trusted relationships and analyse how acquired data can be utilised by all parties in order to create a joint competitive advantage.

How will AI or other new technologies further change cyber defence in the future – both on the defender side and the side of the cyber threat actors, and what does this mean for Europe's security?

Artificial intelligence (AI) will definitely automate a lot of manual processes, whether scanning the networks, finding vulnerabilities, patching, etc. in the cyber domain. Mind that this capability can be applied both in the defensive and offensive mode. It is most certain that Europe needs to further invest in developing AI capabilities, but, most importantly, it must create environments for AI algorithm training. The

bigger the datasets are on which we train our (cyber) AI capabilities, the better these capabilities become. We hear a lot about the supremacy of China in the AI context – note that these kind of centralised governance structures with a smaller focus on privacy enable the creation of enormous datasets for algorithm development and training. Europe has to find its own way on competing in this domain with possibly other supporting technologies, like privacy-enhancing solutions, to provide a serious alternative.

You are part of the consortium developing the European Cyber Situational Awareness Platform through a project co-funded through the EDIDP. How important is this collaborative project for Europe's cyber defence capabilities and European industries?

We are honoured and proud to be part of the European Cyber Situational Awareness Platform development. We believe that one part of the problem in cyberspace is the issue of situational awareness. Namely, how do militaries, governments, and businesses understand their cyber situational posture – what are the assets they own, vulnerabilities and threats they are facing, and what are the risks if something fails or is hacked? Thus, the EDIDP project is of strategic interest to us, both from the content point of view, but also because it provides a unique opportunity to work with different European Ministries of Defence and their cyber units, as well as top national defence companies, like INDRA, Airbus, Leonardo etc. We hope that by the end of this project, countries that we have worked for, will have a cyber situational awareness capability similar to what they have for physical situational awareness today. This, in turn, enables better protection of European troops when deployed on a mission, giving us a competitive edge in conflict situations.

> **"We have good scientific and research potential in Europe"**

What, in your view, is the best way forward for European cyber defence cooperation?

Europe is a unique constellation. We cannot copy our way from anybody else but have to create it through collaboration, trial and error. If we want to be sustainable, we need to collaborate on the creation of our own joint capabilities - whether it is in the domain of a new fighter aircraft, the building of new naval capabilities or in the pursuance of cyber supremacy. We need to plan resources and operate together even when, at times, trust between Member States might not be the highest. The PESCO and EDIDP initiatives are an excellent start for this joint capability building. In the future, we need to enhance this cooperation, see that the projects will not only be part of a small club of companies and that mishaps will not impede our progress. One thing is for sure – when dealing with innovation and creating new structures, mistakes will be made. One needs to learn from these, not walk away from the endeavours.

CYBERNETICA

Cybernetica is an R&D intensive ICT company based in Tallinn that develops mission-critical software systems and products, maritime surveillance and radio communications solutions to over 35 countries across the world.