Cyber webinar
Summary 13.05.2020

“Cyber threats in a pandemic: What’s going on and what is to be done?”

A sharp increase in the number of cyber attacks has been observed since the start of the Covid-19 pandemic. Europe is at peak vulnerability to bad actors while all efforts are focusing on the coronavirus response. This situation is being exploited by cyber criminals and hostile states. In April, the Czech Republic reported cyber attacks on a hospital and airport in Prague while Portuguese energy provider EDP was hit by the Ragnar Locker ransomware. The healthcare sector is particularly targeted. The World Health Organization has reported a fivefold increase in cyber attacks. Some 450 WHO email addresses have been leaked as a result.

It is against this backdrop that the Club of Three held its May webinar entitled “Cyber threats in a pandemic: What’s going on and what is to be done?” with a group of 35 senior figures from business and the policy field in France, Germany and the UK.

The type of cyber attacks perpetrated against critical infrastructures in Europe during the pandemic was a continuation of the hostile campaigns already seen before, but on a bigger scale. The seriousness of the situation was highlighted in a strongly worded Dutch government statement to the UN in which the Netherlands said it was “appalled” by the way some states were using the Covid-19 crisis to launch cyber operations. One participant noted that for countries like Russia, these attacks were part of the hybrid war it had launched since the beginning of the Ukrainian crisis in 2014. Other known actors such as North Korea or China seemed to be driven by opportunism. China in particular was facing accusations by the US of seeking to obtain data on Covid-19 vaccine development. The UK’s National Cyber Security Centre had also raised the alarm over attacks on research facilities.

What could European governments do address these threats? What the Covid-19 pandemic had shown was that Europe needed to urgently and decisively raise its game on cyber defence. Boosting resilience was critical and basic cyber hygiene by European citizens was seen as the first line of defence. One participant pointed out that the use of law enforcement measures such as criminal sanctions could be an effective deterrent against individuals acting on behalf of foreign states. Clear public statements denouncing these activities were also useful tools. Mike Pompeo’s warning following the Czech attacks was described as good practice in this respect and European governments needed to make similar statements. The EU had shown it was capable of taking a more robust approach after reporting in February that it was planning to impose sanctions on entities in Russia and China, as well as several individuals, over cyber attacks.

As owners and operators of critical infrastructures, private companies were instrumental in cyber defence efforts. The challenge for the highly liberalised economies of the West was to find a model that successfully involved multiple private entities in national security plans. Many companies were now seen as national security actors. This had come to light in the US after the authorities moved to reverse the purchase of dating app Grindr by a Chinese company. In Europe, many believed that controlling critical parts of the G5 infrastructure and relying on safe contractors was the best way of addressing concerns over Chinese technology giant Huawei. This was deemed to be a good compromise between a ban and open access, particularly in France. Others however including in Germany still preferred to develop a purely European solution to the G5 question.

After over two decades of operation, the cyberspace was still largely “terra incognita”. In the absence of clear rules at international level, the danger of serious escalations in the cyber domain and beyond was real, especially since the US Cyber Command had taken a more aggressive strategy of persistent engagement. The work conducted within the UN on the development of norms of behaviour seemed to be a good step. These norms could of course be breached and ignored but they had the benefit of setting red lines. Over time, they could help to bring all countries into line. One participant suggested that an agreement between big powers would be needed first, similar to the SALT treaties of the 1970s with conventional weapons, before taking these talks to the UN.