Country: Germany

Committee: DISEC GA1

Agenda Item: Weaponization of Data and Cyber Security

Cyberspace includes all information infrastructures accessible via the Internet beyond all territorial boundaries. In Germany, all players in social and economic life use the possibilities provided by cyberspace. As part of an increasingly interconnected world, the state, critical infrastructures, businesses, and citizens in Germany depend on the reliable functioning of information and communication technology and the Internet. Malfunctioning IT products and components, the break-down of information infrastructures, or serious cyber-attacks may have a considerable negative impact on the performance of technology, businesses, and the administration and hence on Germany’s social lifelines. The availability of cyberspace and the integrity, authenticity, and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has thus turned into a central challenge for the state, business, and society both at the national and international levels. The Cyber Security Strategy is intended to improve the framework conditions in this area. IT threat assessment In recent years attacks against information infrastructures have become ever more frequent and complex, while at the same time perpetrators have become more 2 professional. Cyber attacks are launched both from Germany and abroad. Given the openness and extent of cyberspace, it is possible to conduct covert attacks and misuse vulnerable systems as tools for an attack. In view of technologically sophisticated malware, the possibilities of responding to and retracing an attack are rather limited. Often attacks give no clue as to the identity and the background of the attacker. Criminals, terrorists, and spies use cyberspace as a place for their activities and do not stop at state borders. Military operations can also be behind such attacks. The trend to develop information systems for industry on the basis of standard components and connect them to cyberspace, which is motivated mainly by economic concerns, entails new vulnerabilities. Experience with the Stuxnet virus shows that important industrial infrastructures are no longer exempted from targeted IT attacks. Given the increasing complexity and vulnerability of information infrastructures, the cyber security situation will remain critical also in the future. In Germany, the public and the private sector as well as society at large are all equally affected by targeted or coincidental IT failures. Framework conditions Ensuring cyber security, enforcing rights, and protecting critical information infrastructures require major efforts by the state both at the national level and in cooperation with international partners. Given the shared responsibilities of the state, the industry and the society a cyber security strategy will only be successful if all players act as partners and fulfill their tasks together. The same applies to the international context.

References:

<https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1>

<https://sosafe-awareness.com/resources/reports/human-risk-review/?utm_term=cyber%20protection?utm_campaign=BNLX_ST_WP_Human-Risk-Review-2022_Q22022&utm_campaign=BNLX_ST_WP_Human-Risk-Review-2022_Q22022&utm_source=googlesearch&utm_medium=paid&hsa_acc=2315609737&hsa_cam=16802495493&hsa_grp=136238746318&hsa_ad=591854757806&hsa_src=g&hsa_tgt=kwd-11777710061&hsa_kw=cyber%20protection&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwtIaVBhBkEiwAsr7-c_Mk7QD8ytlp1hQ3z_tKhbASYxnloHkJYAzuXfKWASrD7O1T3YZ8-RoCrgYQAvD_BwE>

<https://www.claranet.de/cyber-security-services/penetration-testing>