BUSINESSEUROPE

STATEMENT

04/10/2018

Cyber-enabled Industrial Espionage

European businesses are increasingly falling victim to large-scale cyber-attacks stemming from non-EU countries aimed at misappropriating sensitive business information such as trade secrets and Intellectual Property (IP). As a result, individual companies suffer irrecuperable damage. Without effective legal means to mitigate cyber-related risks, EU industry as a whole will see its competitiveness impaired and incentives to engage in innovation undermined. Damages resulting from cyber-enabled theft have been estimated to drain between 1-2% GDP[1]. Yet this problem is underestimated and the real damage is likely to be much higher, undermining our economic growth well into the future.

Many EU Member States are grappling with the fast-paced increase in cyber threats, interconnectedness, complexity of the issue and lack of one-size-fits all response. While the right mix of security measures such as security by design in the Cloud, IoT and 5G architecture, IoT certification and strong encryption are good examples of how cyber-resilience could be strengthened, these are very expensive solutions and will never be fully effective without an accompanying strategy to deter hostile actors. In other words, in the cyber world defence is much harder than offence. To this end, BusinessEurope suggests that effective ex-ante and pre-emptive policy responses are considered.

- As a first step, Member States should ensure the **full implementation of the trade secrets Directive**.[2]
- In order to develop our capacities to deter and prevent state funded cyber espionage, the Commission should **launch a study to determine what legal options exist** to deter states engaged in supporting, enabling, tolerating or neglecting the prevention of cyberattacks or cyber-intrusions.
- Finally, alternative non-legal measures such as **diplomatic action or economic retaliation could be considered** as a way to apply pressure on non-cooperative states. China is for instance the one of the state actors that is deemed most problematic in this domain, therefore the EU could seek to cooperate with the United States, Japan and other OECD economies to apply political pressure on countries such as China to cease commercial espionage activities. An agreement within the EU, across the Atlantic and within the OECD as a whole to not to engage in commercial espionage against one another would also deter action from other countries.

* * *

[1] Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies, 2014

[2] Directive (EU) 2016/943

AV. DE CORTENBERGH 168
BE-1000 BRUSSELS
BELGIUM
VAT BE 863 418 279

BUSINESSEUROPE a.i.s.b.l.
WWW.BUSINESSEUROPE.EU
Follow us on Twitter @BUSINESSEUROPE

TEL +32(0)2 237 65 11
FAX +32(0)2 231 14 45
E-MAIL: main@businesseurope.eu
EU Transparency register 3978240953-79