News

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

Avenue des Arts 40 1040 Brussels
www.ecipe.org — info@ecipe.org

ECIPE PRESS RELEASE — NEW OCCASIONAL PAPER

Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?

by Hosuk Lee-Makiyama, Director at ECIPE

Brussels, Belgium, 6th February 2016 - The first-ever study on cyber espionage by foreign governments against European business reveals losses equivalent to 289,000 jobs per year. A new landmark study by ECIPE reveals the extent of commercial cyber espionage against European businesses from government and market intelligence reports.

European and US officials warn that foreign governments are hacking into “everything that doesn’t move” to steal commercial secrets. Europe is securing personal information with all its might, but what about business information?

The risk of hacking is increasing exponentially as 26 billion personal devices, business and industrial equipment are about to become seamlessly connected in Industry 4.0. Within five years, an entire connected business can be copy-pasted, stolen and handed over to a competitor by a government-sponsored hacking group.

While all governments spy, ipso facto. But only a few do so to hand over the information to their industry. Yet it is practically risk-free as government entities cannot be sanctioned under international law, and cyber espionage is undetectable in most cases. It is estimated that 289,000 jobs could be at risk today (ECIPE, 2017). This exposure only increases with digitalisation.

Both the United States and China have already responded to the risks by closing down their markets to each other in critical sectors. Europe is collateral damage in this conflict, and already lost market access in China over national security concerns.

The situation is untenable to Europe. At abroad, market access is increasingly limited due to new cyber security laws. At home, it is affected by cyber espionage, against which it lacks diplomatic, strategic or technical solutions to curb.

In lack of viable options, the report warns of escalating protectionism against China: The scale of the losses is just too big to be ignored, and the targets are “sacred” European manufacturing champions. The EU is proposing security certification on IT products and Union-wide investment screening; The cyber-diplomatic toolbox opens up for sanctions, even in cases when the attacking country cannot be named.

Publication details
Stealing Thunder – Cloud, IoT and 5G will change the strategic paradigm for protecting European commercial interests. Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?, ECIPE Occasional Paper 2/2018

Media contacts
Please contact the author directly at hosuk.lee-makiyama@ecipe.org or +32 499 69 42 49