The threat of state-sponsored industrial espionage

by Massimo Pellegrino

Beijing denies it. Moscow refuses to comment. But, according to Robert Bryant, former US national counterintelligence executive, the governments of both countries are behind efforts to clandestinely acquire industrial secrets, particularly in the realm of cyberspace. In Europe this warning gained little traction. Few governments have complained publicly about such theft. Many businesses preferred to downplay the problem for fear of retaliation. However, this problem can no longer be ignored, and institutions across Europe have finally woken up to the implications of industrial espionage for their national security.

The General Intelligence and Security Service of the Netherlands (AIVD), for example, publicly acknowledged in its 2013 annual report that industrial espionage is a major threat to the economy and that protecting intellectual property and trade secrets is a matter of national security. While traditional national security intelligence gathering was focused on hard security matters, over the past 20 years national and economic security have become indivisible.

Motives and players

Though industrial espionage is as old as industry itself, it has evolved in recent years. First, it has morphed from a small to a larger-scale business. The plethora of information moving over IT networks, the ease of access to cyberspace, and the difficulties in attributing malicious attacks have all contributed to this shift. The second major change is the growing involvement of state actors in targeting non-military technology. Against this new background, Russia and especially China are using industrial espionage to tip the competitive balance in their favour.

There are significant advantages to stealing innovations rather than developing them. Not only can stolen classified material contribute to the development of military and dual-use capabilities, but the money saved can also be reallocated to socio-economic projects.

Motives for state involvement in industrial espionage vary from one country to another. In China, intellectual property rights (IPRs) are not as fiercely defended as elsewhere. Moreover, both the government and businesses often stand to benefit from such actions given that there is very little distinction (if any) between the private and the public sectors. And although China is gradually shifting from being an 'innovation follower' to an 'innovation leader', the slowdown in economic growth is making this process more difficult to fund. Consequently, the clandestine acquisition of necessary technology is all the more tempting. This threat is particularly acute for European companies delivering high-tech goods, which often resort to offshore production and transfer part of their scientific know-how to Chinese partners.

Russian intelligence agencies are in this 'business', too. They operate under a public federal law 'to promote the country's economic development and its scientific and technical progress' and a directive from President Putin 'to protect the economic interests of

Russian companies abroad.' Intelligence gathering is therefore seen (and practiced) as a viable component of the country's modernisation efforts.

Targets and costs

Foreign intelligence services still remain primarily interested in military and defence technologies. The latest generation of Chinese fighter aircraft, for instance, is thought to be based on the F-35 fighter, the blueprints for which were reportedly pilfered from BAE Systems in 2009.

National intelligence communities, however, have also begun to pursue new targets. Examples include research centres and private companies in the fields of aerospace, telecommunications, high-tech electronics, energy, nano- and bio-technology, and financial services. 'Putter Panda', a Chinese People's Liberation Army (PLA) linked group, is believed to have been behind a breach of computer networks of the French National Centre for Space Studies (CNES) in 2012. When the Danish satellite and radio communication firm Thrane & Thrane was hacked back in 2008 – during a wave of attacks dubbed 'Operation Shady Rat' – a group with alleged links to the Chinese government was blamed. And since 2010, 'Dragonfly' (also known as 'Energetic Bear'), identified as a Russian state-sponsored actor, has been conducting espionage campaigns targeting European firms in the fields of electricity generation and energy grid management.

These incidents represent only a small fraction of the thefts which occur. Some estimates say that more than 20% of European companies have been breached, but the actual figures may be much higher. Dmitri Alperovitch, former vice president of McAfee, a US-based security company, maintains that 'firms can be divided into two categories: those that know they've been compromised and those that don't yet know'.

What is happening to this huge amount of stolen sensitive information is still an open question. What is for sure is that the resulting losses can be devastating. A 2014 report jointly released by the Center for Strategic and International Studies (CSIS) and the McAfee Company, for example, suggests that cyber espionage could cost up to 1.5% of a country's GDP. But regardless of the actual figure, steps need to be taken to protect European industry.

Responses and tools

Tackling state-sponsored industrial espionage will require a wide range of tools, as well as efforts to ensure the inclusion of all parties concerned. First, well-crafted competition laws are critical. The 2013 European Commission draft directive regarding the protection of trade secrets against their unlawful acquisition, use and disclosure is a good first step in this direction. However, while the directive calls for goods that make use of stolen trade secrets to be removed from the market, it does not establish criminal sanctions – nor does it clarify whether the matter should be treated differently in cases where those behind the theft are state actors.

Second, international obligations within the framework of the World Trade Organisation (WTO), such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), need to be reassessed. It is no longer practical to adhere to a trading regime in which WTO members are obligated to proscribe theft of intellectual property in their national laws, but are free to engage in it beyond their borders.

Third, a competitive European cybersecurity industry could reduce the damage caused by cyber espionage. The European Cyber Security Protection Alliance (CYSPA) is a promising initiative aimed at increasing the capacity of industry to protect itself from cyber threats. And the European Organisation for Security (EOS), the leading European body representing the private security sector, is well placed to inform policymakers and facilitate dialogue between institutions and the security industry.

Fourth, closer cooperation between the public and private sector might help protect technological and business know-how from theft. For instance, the Italian domestic intelligence agency (AISI) started a programme in 2010 aimed at mapping 100 innovative small and medium-sized enterprises which may need assistance from the intelligence community to guard against the theft of trade secrets. Expanding such efforts and following them up with appropriate training could be coordinated amongst EU institutions to maximise synergies and thereby allow for the implementation of effective protection strategies with limited resources.

Finally, working with international partners affected by similar problems may help develop joint plans. The EU-US Working Group on Cybersecurity and Cybercrime has been an important forum for identifying common strategic goals and taking concrete actions. Such efforts should continue and be directed towards ensuring the inclusion of legally-binding principles against industrial espionage in the Transatlantic Trade and Investment Partnership (TTIP). Achieving all this will require hard diplomatic graft: but just as espionage is global in nature, so, too, are the answers to it.

Massimo Pellegrino is a Junior Analyst at the EUISS.

 | QN-AL-15-026-2A-N | ISBN 978-92-9198-321-6 | ISSN 2315-1129 | DOI 10.2815/184955