Occasional paper
No. 2/18

Hosuk Lee-Makiyama
Director of European Centre for
International Political Economy

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

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?

55 billion euros lost annually to cyber espionage.
289,000 jobs at risk.
No workable solutions.
26,000,000,000 new devices soon to go online.

Executive Summary

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?

- Information like ongoing contract negotiations, customer and marketing data, product designs and R&D are commonly uploaded to the cloud already today.
- 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. Spying is highly lucrative, especially for emerging countries.

- Verified historical data (IZA, 2017) shows the gains are substantial, equivalent of boosting exports to Europe by 30% even in the pre-internet era (ECIPE, 2017).
- Yet it is practically risk-free as government entities cannot be sanctioned under international law, and cyber espionage is undetectable in most cases.
- While Europe is one of the worst protected IT environments (Deloitte, 2016), it possesses the know-how in the sectors most attractive to emerging countries, like motor vehicles, biotech, infrastructure equipment, aerospace.

• It is estimated that 289,000 jobs could be at risk today (ECIPE, 2017). This exposure only increases with digitalisation – and by 2025, the losses is equivalent to a million jobs.

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.

• China has concluded treaties to end commercial cyber espionage with the US and its allies in the Five Eyes intelligence alliance, with considerable resources for cyber deterrence – while shunning Germany and other EU countries who are unlikely to develop such capabilities.

• 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.

Europe will have no choice but to use the only option at its disposal: Disrupt China's access to the Single Market to create a negotiation leverage.

• Legislative processes for EU-wide investment screening and product certification and stricter security screening of ICT vendors in some Member States are already in the works.

• Whether these measures help to secure European corporate data is secondary to the economic leverage it creates. By Europe's moral imperative, it is China's strategic choices that pushed the EU to the point of no return – thus, it is China's responsibility to de-escalate the situation if it wants to keep the EU markets open for Chinese exporters.

Introduction: Digitalisation, statecraft and espionage[1]

THAT CYBERSECURITY IS A SERIOUS TOPIC in international economics will need no justification by 2025. However, at the time of writing – late 2017 – it may require a contextualisation to why commercial espionage is an economic issue for Europe. This study estimates that commercial cyber espionage puts up to €60 bn in economic growth and up to 289,000 jobs at stake in the EU. The backdrop to this emerging crisis is the ever so fierce competition for global market shares and innovation between the world's major powers. As we are a decade into the pivot to Asia, foreign policies of China and the US are blatantly driven by commercial objectives, and economics are shaping the strategic landscape. Emerging powers are putting economics at the centre of their foreign policies".[2]

In today's economic statecraft, firm-level commercial interests are supported by government agencies, and cyber espionage is a central part of the policy toolbox. Senior US officials have warned that foreign powers are "trying to hack into everything that doesn't move in America. Stealing commercial secrets … from defence contractors, stealing huge amounts of government information, all looking for an advantage."[3]

Since the East India Company of the 16th Century, the collusion between power and commerce has always been a fact of life – and internet is just a new chapter in that evolution. Just to mention two examples, a Chinese group (with alleged ties to People's Liberalisation Army) conducted industrial espionage on thousands of western firms during 2009[4]. The incident, called Operation Aurora in western media, implied an unprecedented degree of state and business collusion and targeted relatively ordinary business (such as banking and chemicals) rather than military intelligence. Moreover, Prism program of National Security Agency (NSA) made use of commercial over-the-top (OTT) services to eavesdrop on information, and targets include elected European officials.

All Governments spy, albeit for different reasons, but only a few do so for commercial motives, to pass on the acquired knowledge to their own companies. While the EU has used almost its entire political bandwidth in pursuit for privacy protection against the NSA and Silicon Valley, it heeds less to the warnings against industrial espionage, where tactical business information online concerning ongoing contract negotiations, customer information and intellectual property may be targets. Ultimately, resilience against cyber espionage is about integrity and confidentiality of the data for businesses, in the same manner as privacy protection for individuals.

How cyber espionage disrupts commerce

AS THE ASIAN COUNTRIES have quickly caught up with the West in the ICT sector, the developed and emerging countries are ever-closer on the world's technological frontier. Shrinking the digital divide that leads to more inclusive trade and open market competition is a thing of good – or even the ultimate goal for a free trader. However, there is more besides the free and friendly

[1] This report stands on the shoulders of the work by CSIS, IZA, Council of Foreign Relations, the Directorate General for Safety and Security (DGV) at the Ministry of BZK of the Netherlands, and the German Federal Ministry of the Interior. The author also wishes to thank the assistance of Valentin Moreau and Nicolas Botton, as well as the invaluable comments by Martina Ferracane, Bruno Macaes and European officials who have shared their insights.

[2] Clinton, H R, Delivering on the Promise of Economic Statecraft, Remarks on November 17, 2012

[3] Becker, A, Hillary Clinton accuses China of hacking U.S. computers, Reuters, July 5, 2015, accessed at: https://www.reuters.com/article/us-china-usa-clinton/hillary-clinton-accuses-china-of-hacking-u-s-computers-idUSKCN0PE0TI20150705

[4] Cha, Nakashima, Google China cyberattack part of vast espionage campaign, experts say, Washington Post, January 14, 2010, accessed at: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

competition by legitimate means. Government interference, subsidies and protectionism have led to market distortions and inefficient allocation of resources.

As over 50% of global trade in services is enabled by ICT technologies[5], information technology is the modern equivalent of shipping lanes or synaptic nerves that tie any global organisation together. If technology is the enabler of economic statecraft, telecommunications and online services are its most vital assets. The cloud and next-generation broadband have already enabled online storage. Business deposit and share tactical information on ongoing contract negotiations, customer data or technical description of product designs, business processes and ongoing R&D in their networks. Moreover, all files and data available on devices, servers or workstations are universally accessible from the corporate network, and also accessible from the public internet, albeit via virtual and encrypted private networks (VPN). Practically no corporate network maintains a physical "air gap" to the internet, making access to the vital corporate information physically inaccessible from public networks.

Three weeks of disruption is sufficient to erase the annual profit margin and shareholder dividends for a typical, publicly traded German company

Furthermore, even the smallest SME host their financial systems for accounting, payments and inventory online. So are business support systems for point-of-sales, marketing, R&D and operational planning used by each function of a firm. Today's cash registers are actually PCs that are interconnected via the open networks to the head office functions, aggregating information all the way up to the chief financial officer, or the CEO, or into the customer database in the marketing department.

This corporate infrastructure makes them vulnerable to not just economic espionage and theft, but also to disruptions. Malware (which corrupts system information) still accounts for the most common type of breaches, and particularly ransomware, a type of malware like WannaCry that triggered the first intra-EU operational cooperation under the NIS directive.[6]

On an average week of the year, one week of business disruption reduces corporate turnover by 2%. Given that the 110 largest German companies had margins of just 6.3%[7], three weeks of disruption is sufficient to erase the annual profit margin and shareholder dividends for a typical, publicly traded German company. Not even the crisis-resilient manufacturing companies of the German Mittelstand survive more than three weeks and five days on an average,[8] withstanding costs for restoration of systems and data.

Today, 96.5% of all SMEs in developing economies store some form of business data digitally.[9] A considerable amount of intellectual capital and know-how is already digitised and stored online.

---

[5] UNCTAD, ICT Economy Report, 2011

[6] Council of the European Union, Cybersecurity - Information from the Commission, May 31, 2017

[7] Weber, W.W, Germany's Midsize Manufacturers Outperform Its Industrial Giants, Harvard Business Review, August 12, 2016, accessed at: https://hbr.org/2016/08/germanys-midsize-manufacturers-outperform-its-industrial-giants

[8] ibid.

[9] Zurich, Potential effect on business of small and medium enterprises (SMEs) due to cybercrime in 2016, November 2016

Europol warns that most, if not all, public-facing critical infrastructure sectors rely extensively on computer systems for many aspects of their industry.[10] One in five industrial computers is attacked every month,[11] and Europol observes an upsurge attributed to not common cyber-criminals but advanced persistent threat (APT) groups with a new geographic distribution – most notably in Asia (i.e. China and to a lesser degree North Korea).[12] Although there is a risk of high impact attacks, they are almost universally becoming more prevalent each year, relying heavily on social engineering tactics such as spear-phishing to convince individuals within the target company to breach or circumvent their own IT security measures. Moreover, the manufacturing sector remained among the top 3 industries targeted by spear-phishing attacks,[13] while the number of vulnerabilities found in industrial control systems in the world quadruped in a single year.[14]

"An entire connected business can be copy-pasted and stolen".

Exponential risk from Industry 4.0

TODAY'S FIBRE-BASED FIXED-LINE and 4G/LTE and cloud architecture connects billions of devices and already hosts much of business assets. However, the next generation of networks is already at the door – with new risks and threats that must be mitigated.

Market forecasts predict that the number of connected devices in the world would more than triple in just three years with the evolution of Internet of Things (IoT) where 26 billion business equipment, personal devices and household items go online.[15] The biggest shift from the fifth generation of mobile services (5G) does not come from its capacity of 200 times faster speeds, 1000 times better energy efficiency or 20 times shorter latency[16], making it suitable for an infrastructure for manufacturing and business services – but from what a 5G mobile network actually enables.

5G is the first generation of mobile network that is primarily designed for businesses and industrial equipment, merely offering new speeds to consumers as a residual service. As more and more corporate data migrates to the cloud through connected business, seamlessly integrating manpower, machinery and equipment through a high-speed 5G network, today's information processing and data storage can take place on the field in real-time. In effect, the entire company and its customers are virtualised, interlinked and monitored to enable the Fourth Industrial Revolution.

Commercial cyber espionage today provides transgressors with information on production formula for a new chemical compound, or what the competing bids are. This is by and large the same kind of information that commercial espionage could provide in the old days of human and traditional signal intelligence. The next-generation Internet and the Industry 4.0 are taking the problem to a new level – not just documents and trade secrets such as product design, but

[10] Europol, Internet Organised Crime Threat Assessment (IOCTA), 2017

[11] ibid.; Kaspersky Lab, 2017, Threat Landscape for Industrial Automation Systems in the Second Half of 2016, p10.

[12] Ibid.; Symantec, 2017, Internet Security Threat Report: Volume 22, p 15, April 2017

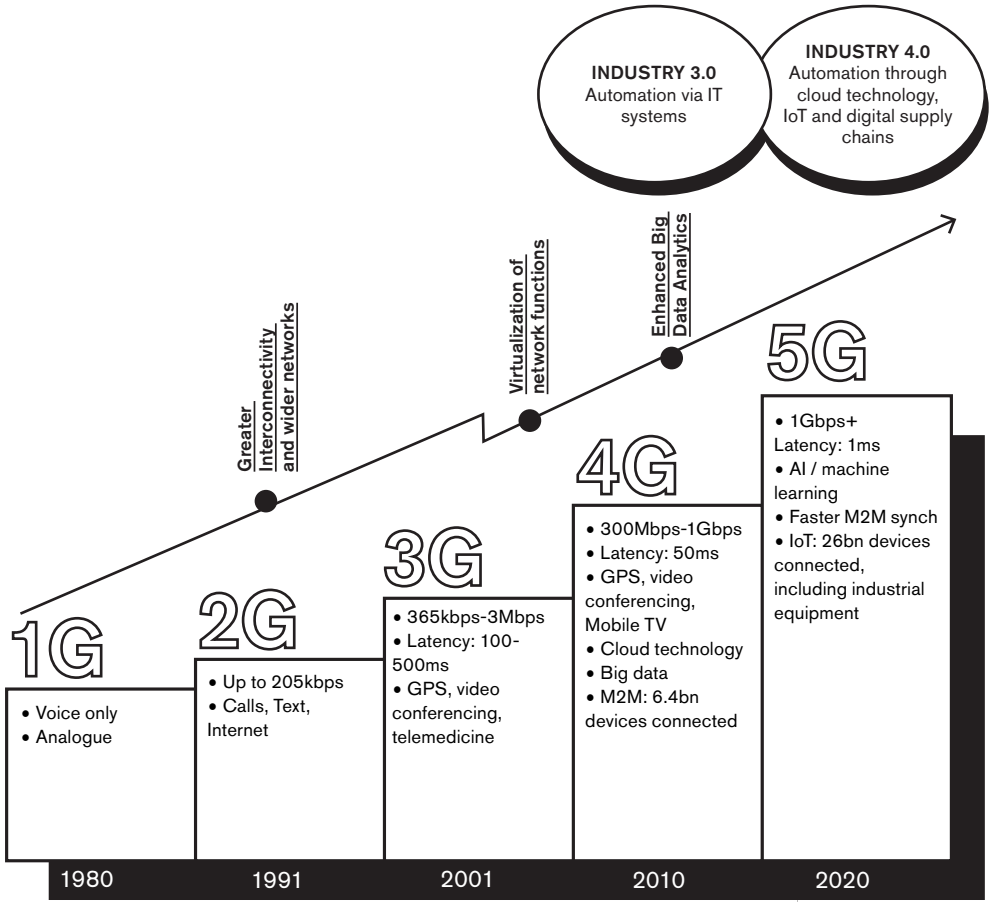
[13] Symantec, Internet Security Threat Report: Volume 21, p41, April 2016

[14] ibid.

[15] Gartner, Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2016; Rentzhog, M, No transfer, no production, National Board of Trade of Sweden, Rentzhog, No Transfer, No Production, 2015

[16] IHS Economics and IHS Technology, The 5G economy: How 5G technology will contribute to the global economy, January 2017, accessed at: https://www.qualcomm.com/documents/ihs-5g-economic-impact-study

Evolution to 5G, IoT and Industry 4.0



Source: Waslo, Lewis, Carton (2017)

an entire connected business can be copy-pasted and stolen, including equipment settings, operational schedules and production details.

Industry 4.0 – with its digital supply networks, smart factories and digital manufacturing – brings new risks and threats for smart manufacturers and digital supply networks.[17] Even with proper contingency plans, decades of R&D can be stolen within a few minutes. Once penetrated, hackers do not even need the secret blueprints, formulas, recipes, business plans – they can see how an entire connected and autonomous business, or its production process is run from within. Location of transport equipment and shipments disclose markets where the company is vulnerable and is running low on supplies. Strategic correspondence or geolocation data of key management could reveal the names of important ongoing business, or potential customer losses. This is in addition to what is already often stored on the cloud today in the form of customer data, contracts, IPRs or prices where the changes may be observed second by second, rather than day by day or week by week.

[17] Waslo, Lewis, Hajj, Carton, Industry 4.0 and cybersecurity, Managing risk in an age of connected production, March 21, 2017, accessed at: https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

Already in 2010, the incidence of electronically stolen data surpassed that of physical theft,[18] and the volume of data that can potentially be accessed and stolen keeps growing exponentially. Not surprisingly, the European Commission estimates that the total value of data markets should increase by 2.6 times and reach at least 5% to EU GDP by 2025 (against 1.87% in 2015). The amount of data created will continue to increase and should be multiplied by eight between 2016 and 2025 (from 20 to 160 Zettabytes). It is not unreasonable to assume the value of corporate assets stored (and thereby exposed to the EU cost of cyber espionage) will increase proportionately by 2.6 to 8 times today's values.

The legality of state-sponsored commercial espionage

ALL SOVEREIGNS SPY, IPSO FACTO. The internet has provided a cost-efficient means to build intelligence capabilities in signal intelligence that were too costly aside for the world's superpowers in the past. This has in turn considerably levelled the playing field between small and big powers, and consequently, all governments spy on adversaries, and sometimes on allies; they spy on other governments, individuals and businesses.

However, as nearly all the digital infrastructure is owned by deregulated commercial actors, cyber espionage requires the coerced participation of those who run or manage the digital services for signal intelligence, or human intelligence from business partners. For example, several NSA programs including PRISM, BLARNEY and Xkeyscore utilised the access to social media, streaming and email services. Similarly, a report by Mandiant (a leading forensic investigation firm) made the case that 100 intrusions into commercial companies could be traced to a branch of Chinese government – an entity known as "Unit 61398" within the China's People's Liberation Army (PLA) – and not just hired freelance groups.[19]

The examples of the US and China seem to suggest that collaboration between state and non-state actors on cyber espionage is least tacit and may be common practice. However, the purpose of the espionage differs distinctively between the cases, which also has a bearing on their legality under international customary law. For instance, legal expertise deems that cyber *espionage* (unlike a destructive cyber-*attack*) does not violate international law *per se*,[20] proviso the objective is entirely non-*commercial*.

There are cases where governments may spy on businesses without any intent of exploiting the information to gain a commercial advantage – for example, to monitor compliance with UN sanctions, verify statements of financial institutions that could destabilise the global financial system, or monitor activities in strategic sectors like aerospace and energy. The practice only turns illicit if the result of the spying is passed on to a private or public entity for competitive advantage – i.e. the very definition of *commercial* cyber espionage.

The cooperation between commercial entities and governments is incentivised by several factors, including its uncertain standing within international law. One interpretation could be that state actors enjoy immunity for non-commercial cyber activities from other jurisdictions,

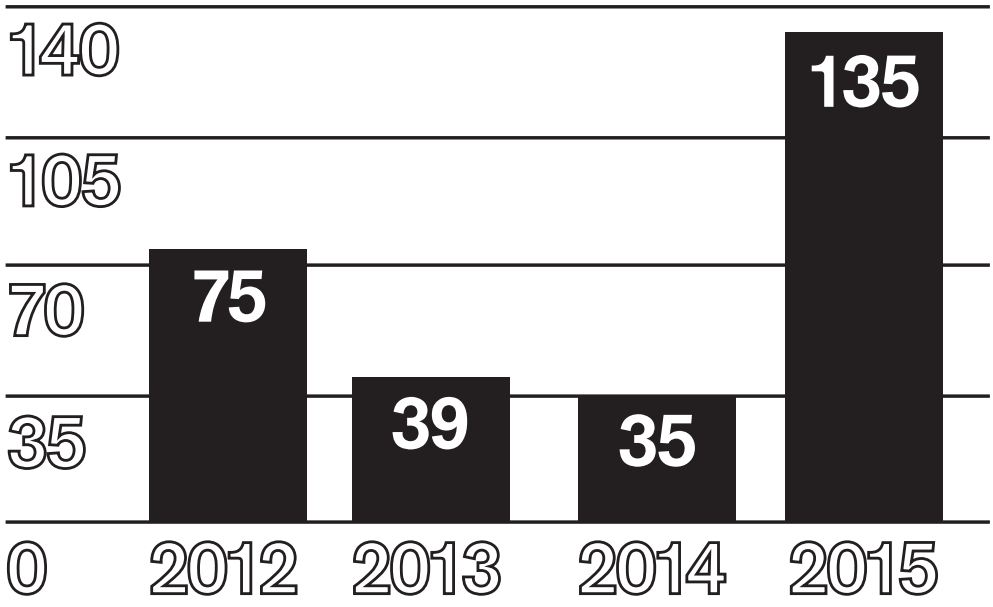
---

[18] Global International, Global Fraud Report 2009-2010, accessed at: http://www.kroll.com/CMSPages/GetAzureFile.aspx?path=~%5Cmedia%5Cfiles%5Cintelligence-center%5Cglobal-fraud-report-2009-2010-english.pdf&hash=f30b40b550edf60faa044219623d7815240415b866603e0310c6838142c86582; Alphr, Stolen data most costly theft for companies, October 18, 2010, accessed at: http://www.alphr.com/news/security/362026/stolen-data-most-costly-theft-for-companies#ixzz12j0BpRnE

[19] Mandiant, APT1 Exposing One of China's Cyber Espionage Units, 2013,

[20] Radsan, J, The Unresolved equation of espionage and international law, Michigan Journal of International Law, Volume 28, Issue 3, 2007, accessed at: http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1170&context=mjil

Vulnerabilities disclosed in Industrial Control Systems



Trend towards Vulnerability and Future Risks

IoT
Higher inter-connectivity and greater amount of connected devices means more opportunities for breach.

Data
Greater reliance on data and the digitization of processes means that information becomes easier to steal.

Cloud
widening networks relying on single platforms means that attacks will have larger scopes.

Open systems
Industrial systems striving for greater openness and accessibility within a firm network ultimately create more avenues for attack via IP addresses.

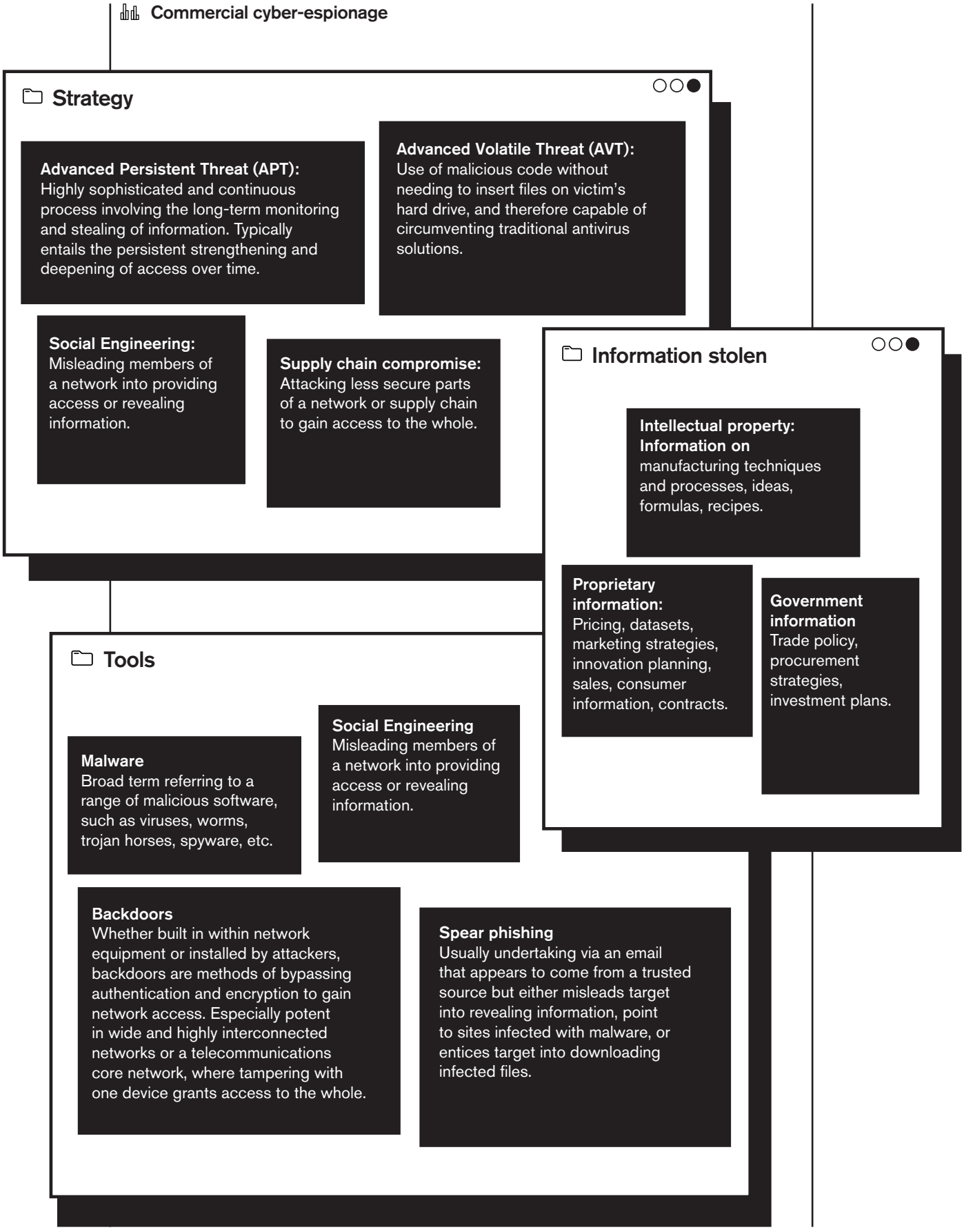
Source: Symantec, 2016: Verizon, 2017

and all military cyber infrastructure – e.g. a command centre, or surveillance facility – therefore must fall within that immunity.[21] Moreover, actions of state-sponsored group, including so-called "advanced persistent threat" (APT) groups or state-owned enterprises could be attributable to the state, and thereby under immunity.

However, commercial espionage is not just feasible – it is also highly lucrative. A recent study, by IZA Institute of Labor Economics of Germany,[22] conducted on actual cases of state-sponsored commercial espionage found in the East German state archives showed that East Germany managed to close its productivity gap with West Germany by 6.3 percentage points by 1989. East Germany used espionage as a productivity improvement measure that was far more cost-efficient than investing in their own indigenous R&D. The same productivity multiplier today would give a country like Russia an annual GDP boost of €12bn, while China would increase GDP by €96bn, which is equivalent to increasing the country's exports to Europe by 30%. If East Germany achieved such economic productivity boosts even during the pre-digitalisation days, it is self-evident that commercial cyber espionage provides a competitive gain that is manifold today.

[21] See Rule 12, paras 2. and 8 of Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

[22] Glitz, Meyerson, Industrial Espionage and Productivity, IZA, IZA DP No. 10816, June 2017


Commercial cyber-espionage
Strategy
Advanced Persistent Threat (APT): Highly sophisticated and continuous process involving the long-term monitoring and stealing of information. Typically entails the persistent strengthening and deepening of access over time.
Advanced Volatile Threat (AVT): Use of malicious code without needing to insert files on victim's hard drive, and therefore capable of circumventing traditional antivirus solutions.
Social Engineering: Misleading members of a network into providing access or revealing information.
Supply chain compromise: Attacking less secure parts of a network or supply chain to gain access to the whole.
Information stolen
Intellectual property: Information on manufacturing techniques and processes, ideas, formulas, recipes.
Proprietary information: Pricing, datasets, marketing strategies, innovation planning, sales, consumer information, contracts.
Government information Trade policy, procurement strategies, investment plans.
Tools
Malware Broad term referring to a range of malicious software, such as viruses, worms, trojan horses, spyware, etc.
Social Engineering Misleading members of a network into providing access or revealing information.
Backdoors Whether built in within network equipment or installed by attackers, backdoors are methods of bypassing authentication and encryption to gain network access. Especially potent in wide and highly interconnected networks or a telecommunications core network, where tampering with one device grants access to the whole.
Spear phishing Usually undertaking via an email that appears to come from a trusted source but either misleads target into revealing information, point to sites infected with malware, or entices target into downloading infected files.

As the East German example shows, commercial espionage is a cost-efficient shortcut for global competitiveness, which in turn brings growth and jobs that are critical for popularity and legitimacy of incumbent governments. This is particularly true for export-led countries in Europe or Asia, which are also mixed economies with conflation of private and public objectives. Strong economies project strategic influence and power at home and abroad – and it is not without reason that commercial cyber espionage is an established part of economic statecraft.

The absence of smoking guns

WHILE THE RETURNS OF COMMERCIAL ESPIONAGE are increasing, the means of espionage and risks of attribution are diminishing. Attributions (so-called smoking guns) are nearly non-existent. An assessment by the Dutch Minister of the Interior acknowledges that economic, strategic, technical and scientific espionage is possible due to increasing number of ways of intercepting fixed and wireless communications. The integrity of the information cannot be guaranteed when foreign party's telecom network is used for interconnectivity,[23] or due to the "large-scale purchasing of technical equipment, outsourcing to third parties and offshoring of ICT functions".[24] If the equipment in a company network (or the core or access networks of a national telecom infrastructure) has been tampered with or has backdoors with "unpublished features" would allow for unhampered interceptions, control or degradation of the network, entirely unnoticed. While the Dutch intelligence service claims to have "substantial indications that foreign intelligence services are interested in information on the Dutch telecom network,"[25] they can do so without risk of being identified. The Dutch government report does not preclude that states may coerce vendors in their jurisdiction or even establish vendors solely for the purpose of acquiring information.[26]

Even less resourceful non-state actors can act without any risk of attribution as internet was never engineered to be traceable, and allocates dynamic (i.e. temporary and changing) IP-addresses to connected devices. Moreover, these addresses can be cloaked, falsified or multiple hacked user accounts can be used to hide any traces. Even in the unlikely case that the host country assists in tracing the origin of an attack, the identification of the computer and its location does not reveal the identity of the attacker, and activities of threat groups are likely to be sanctioned (or at least unpunished) by their host governments.

All sovereigns spy, *ipso facto.*

Europe's vulnerability to cyber espionage

DESPITE THE FACT THAT the EU is not in a geopolitical standoff with neither the US nor China in the Asia-Pacific, it is still entrenched in a fierce global commercial competition on the export markets with both. Firstly, although the EU and its Member States pose no direct geopolitical threat to either the US nor China, Europe has been inevitably drawn into their détente. EU firms have already lost sizeable share of their market access on digital goods and services in China (and continue to do so) as they are more often than not automatically treated on par with the US,

[23] General Intelligence and Security Service of the Netherlands (AIVD) and the Directorate General for Safety and Security (DGV) at the Ministry of BZK, Analysis of vulnerability to espionage, 2011

24 ibid.

25 ibid.

26 Ibid. Ch 8.5

Cases of state-sponsored commercial espionage found in the East German state archives showed that East Germany managed to close its productivity gap with West Germany by 6.3 percentage points

Japan and other strategic adversaries to Beijing according to the most-favoured nation principle. [27]

Secondly, there is no evidence or indication that cyber espionage against European firms is any lesser in scale than against other countries. While Europe sits on very attractive know-how in manufacturing, European countries are among the least protected security environments in the developed world, making Europe a honeypot of corporate espionage. Several EU countries (including Germany, the UK, the Netherlands, Denmark, Finland and Sweden) belong to countries with the weakest cyber defences and six times more vulnerable than other countries.[28] Germany's Bundesamt für Verfassungsshutz (the Intelligence Service charged with upholding the constitution) boldly claims that "Chinese intelligence services focus on industry, research, technology and the armed forces (structure, armament and training of the Bundeswehr, modern weapons technology)."[29]

Germany's finger-pointing at China could be the results of research bias. After all, if German law enforcement agencies look for evidence of Chinese commercial espionage, they are not very likely to find French activities. There are also less ominous and natural explanations: Europe tends to lead in those light manufacturing sectors that are of interests to emerging countries in their next step of development. Even if all nations spied for commercial objectives, countries who are ahead of Europe in the technology curve have much less to gain from stealing Europe's thunder.

Meanwhile, China designates certain industrial sectors as strategic emerging industries (SEIs) in its industrial policy that is planned in five-year cycles. From 2016 onwards, the Chinese leadership has also decided that these emerging sectors should account for no less than 15% of China's GDP at the end of the new period. Expert witnesses claim that foreign firms in the SEI sectors of the 12th Five-Year Plan are more likely to be targeted by hackers sponsored by the Chinese government.[30] The 12th Five-Year Guideline for National Economic and Social Development for 2011-2016 named several European export interests as China's new SEIs.[31] In addition, electric and hybrid vehicles were added with 5G, artificial intelligence (AI) and IoT technologies in the 13th plan for 2016-2020.

European governments traditionally advocate better R&D protection through advocacy of international treaties (such as trade agreements, TRIPS in the WTO, and WIPO treaties) as IPRs cannot be protected unilaterally. The EU cannot enforce its IPRs overseas unless the jurisdiction in the country has a similar set of rules and its courts are inclined to rule in Europe's favour.

---

[27] Ferracane, Lee-Makiyama, China's technology protectionism and its non-negotiable rationales, ECIPE, 2017, accessed at: http://ecipe.org/publications/chinas-technology-protectionism/

[28] Deloitte, Global Defense Outlook 2016, accessed at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/public-sector/ca_en_ps_global_defence_outlook_2016_interactive_AODA.PDF

[29] German Federal Ministry of the Interior, Brief Summary 2016 Report on the Protection of the Constitution, 2016, accessed at: https://www.verfassungsschutz.de/embed/annual-report-2016-summary.pdf

[30] Weedon, J, Testimony before the U.S.-China Economic and Security Review Commission, Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China, Washington, DC, June 15, 2015, accessed at: http://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf

[31] Lee-Makiyama, H, Chasing Paper Tigers, ECIPE, 2011

However, most commercially relevant research cannot be patented. Whereas Europe on a policy-level continues that tradition by calling for protection of what it calls "trade secrets", but any kind of IP theft remains hard for firms to detect, much less obtain legal redress for. Therefore, businesses rely on their own efforts to conceal trade secrets and less on patents that entail public disclosure.[32] US official reports quote estimates suggesting that the value of trade secret theft is between 1% and 3% of GDP, meaning that the cost to the $18 trillion U.S. economy is between $180 billion and $540 billion.[33]

Furthermore, US official reports claim IP protection costs "have skyrocketed, especially in response to cyber-enabled IP theft", and there are no indications of the cost to Europe being any less. In response, a recently launched EU Cyber-Security package signals an increased European ambition in the cyber-security domain.[34] Nonetheless, any actions on cyber espionage targeting businesses are out of its scope, despite the fact that espionage accounts for at least quarter of all cyber incidents and majority of the costs.[35]

The cost of cyber espionage to Europe: 289,000 jobs

WITH INCREASING THREATS, the spending on cybersecurity solutions (such as firewalls and threat intelligence) by governments and the private sector is rising steadily with estimates showing the cost is approaching 0.1 percent of global GDP.[36] Some researchers even claim that the risks and costs of cloud and 5G already outweigh the gains of digitalisation.[37] However, such Luddite approach – to unplug the cables and attempt to stop digitalisation would not help, as it would simply keep the costs and remove the gains, and put Europe comparatively worse off against international competition.[38]

Aside from preventive costs, cyber espionage and other cybercrimes have a direct negative impact on businesses (business disruption, information loss, revenue loss, equipment damages, reputational loss that, in sum, decreases the potential to innovate due to a potential threat of theft by reducing the rate of return to innovators and investors.[39] It is thus a direct threat to companies' productivity since it negatively impacts technical progress.

A 2014 analysis by the CSIS put the global cost of cybercrime up to $575 billion annually, or 0.8% of global GDP. Within the European Union, the cost of cybercrime is estimated at 0.41% of GDP or 55 billion euros in the year of the study. Another study by the leading underwriters of the insurer Lloyd's,[40] estimated that one single cloud service disruption scenario could lead to dramatic economic losses ranging from US$4.6 billion for a major event to US$53.1 billion for an extreme event (0.07% of global GDP in 2016).

---

[32] Halligan, R M, Trade Secrets v. Patents: The New Calculus, Landslide, July/August 2010

[33] Center for Responsible Enterprise and Trade (CREATe.org) and PwC, Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats, 2014

[34] European Commission, Regulation on ENISA and the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017)477, 2017

[35] Verizon, 2017 Data Breach Investigations Report, 2017, accessed at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[36] CSIS, The Economic Impact of Cybercrime and Cyber Espionage, July 2013

[37] Atlantic Council, Zurich Insurance Company Ltd, Overcome by cyber risks? Economic benefits and costs of alternate cyber futures, 2015, accessed at: http://www.atlanticcouncil.org/images/publications/risk-nexus-september-2015-overcome-by-cyber-risks.pdf

[38] Bauer et al., ECIPE, 2014

[39] Jim Lewis, Senior Fellow and Director of the Strategic Technologies Program at CSIS, "Cybercrime is a tax on innovation and slows the pace of global innovation

[40] https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report

List of advanced persistent threat (APT) groups and incidents targeting EU interests

Incident, threat group	Alleged government sponsor	Year	EU interests affected	
APT 10	China	2017	UK, FRE, SWE, FIN	The Chinese group APT 10 a.k.a. Red Apollo has been stealing intellectual property, and other sensitive data from several managed IT service providers and their customers, which included **energy, finance, technology, and healthcare** firms since at least 2009. A clear example of commercial rational involved the targeting of **Solar World**, a German firm, which saw sensitive manufacturing, production and cost data stolen at a time when Chinese manufacturers of solar products sought to enter US markets.
OPERATION BUGDROP	Russia	2017	AUS	Operation BugDrop was a Russia-sponsored cyber-reconnaissance mission which gathered intelligence about targets in various domains including **critical infrastructure, media, and scientific research.** It concerned the capture of a range of sensitive information from its targets including audio recordings of conversations, screenshots, documents and passwords.
"OCEAN LOTUS"	Vietnam	2015	GER	Ocean Lotus is a group backed by the Vietnamese government which used its access to private sector data for law enforcement, intellectual property theft and anti-corruption measures that could be used to erode the competitive advantage of the organisations targeted. It targeted mostly foreign firms with interest in Vietnam's **consumer products, manufacturing, hospitality, network security, technology infrastructure and banking** sectors.
UPS	China	2015	UK	UPS is a China-sponsored phishing operation which targeted **aerospace, defence, construction, engineering, technology, telecommunications and transportation firms**
EMISSARY PANDA	China	2015	UK, FRA	Emissary Panda, a Chinese operation, targeted **aerospace, automotive, technology, and energy** sectors, **manufacturing** data and together with defence and political intelligence, Possible commercial motivations include theft of competitor capabilities, pre-empting of innovations and financial or pricing movements, and competitor development plans.
"AXIOM"	China	2014	UK, GER, NED, BEL, ITA	Axiom, a Chinese group, has targeted organisations that are of strategic economic interest in **technology, telecommunications, infrastructure environmental and energy** policy. Its activities fit within the Chinese plan to wane themselves off foreign technology and have their own capabilities catch up with competitors.
"CARETO"	Spain	2014	UK, FRA, ESP, GER, POL	Careto is a threat actor who is probably sponsored by Spain and which has targeted **energy, oil and gas companies**, research institutions and private equity firms. Its malware is very sophisticated and has the potential to intercept all communication channels and collect any vital information from its target.
"CROUCHING YETI"	Russia	2014	ESP, GER, FRA, ITA, IRE, POL	Russian backed Crouching Yeti has spied on a number of sectors **(pharmaceuticals, health, automotive, network infrastructure, IT)**, and furthermore had the potential to be used for sabotage.
PEOPLE'S LIBERATION ARMY	China	2014	SolarWorld	Five officers of the People's Liberation Army were indicted by the US for targeting the **metal industry, nuclear and solar power industries,** including the US subsidiary of the German firm SolarWorld. Purpose was to steal information that could be used by Chinese competitors.
PEOPLE'S LIBERATION ARMY UNIT 61398	China	2013	UK, FRA, BEL, LUX	China's Unit 61398, or APT1, has targeted 141 companies spanning 20 major industries, including **IT, transportation, technology, financial services, engineering, chemicals, energy, and healthcare**, all of which are related to China's strategic priorities.
COMPROMISE OF EADS (AIRBUS) AND THYSSENKRUPP	China	2013	EADS/Airbus ThyssenKrupp	The compromise of **ThyssenKrupp** by Chinese hackers was most likely out of commercial interest, as it is a major player in the global steel industry. Additionally, the commercially essential intellectual property stolen from **EADS (now Airbus)** concerned design plans, aerodynamic calculations and cost estimates.
"NITRO ATTACKS"	China	2011	UK, GER, CZE, NED, FIN, FRA	The Chinese sponsored Nitro attacks concerned private companies in the development and manufacture of **chemicals** and collected intellectual property (design documents, formulas and manufacturing processes)

Source: Council on Foreign Relations, Cyber Operations Tracker, accessed at: https://www.cfr.org/interactive/cyber-operations

This is the cost of one extreme event which means that if multiple incidents of such scale happen within one year, the annual global cost might be higher. The potential economic damages due to an extreme cyber-attack event could be as significant as those caused by major hurricanes.

However, attacks are not isolated "incidents" but a constant evolution that could go undetected for years. Moreover, there is a considerable number of undisclosed or undiscovered incidents. Estimating the societal cost of cyber espionage comes with several methodological challenges. Estimating the value of the knowledge stolen and the opportunity cost of that information given to a competitor is difficult to appraise – and incident and its costs are often never known to the target at all. Unlike cases of fraud or disruptions that are one-time costs, espionage creates dynamic costs over the years through lost competitiveness and market shares.

The actual cost of commercial cyber espionage does not arise from the hacking itself but when the acquired knowledge is transferred to commercial interests. Commercialisation of the new ability is thereby used to displace foreign competition on the home and world markets. The consequential loss in revenues and profits is defined by the commercial value of the foreign comparative advantage defused. Therefore, the economic damage on Europe from commercial cyber espionage could be significantly larger than modelled. Hence, the substantial part of the costs arising cybercrime can be attributed to cyber espionage, CSIS and others essentially equalise these costs, although the data points are subject to considerable uncertainties and generalisations in their assumptions.[41]

The economic impact estimated in these reports cover a range that could offset the gains achieved through a medium-sized FTA (e.g. EU-Korea) or major gains we would have seen from TTIP or the completion of the Single Market. It threatens global trade, especially at a time when most transactions depend on secure communications.

In the long-run, this net loss in GDP that stems from loss of competitiveness and subsequent decreased industrial output will cause a rise in the unemployment rate. There is a definite correlation between growth and jobs, which is subject to years of economic research of their statistical relationship, (so-called Okun's law) for each economy.

The most recent economic crisis of 2007-2010 provides the most recent data on how European labour markets contract following destruction of corporate assets and lower outputs. 289,000 potential new jobs are lost due to cyber espionage across the EU.[42] Other long-term estimates implicate a loss of 600 000 jobs in the European Union.

Actual economic losses could be lower or higher than the average in the scenarios because of the uncertainty around the number of incidents per year, or factors such as the organisations involved, or how long the disruption lasts. In addition to the significant job effects, there are job losses due to the protectionist measures imposed by other countries. Over time, these incidents will become more common as the technology involved in cyber espionage is dispersing to new actors. NSA has acknowledged that cyberweapons developed by the agency have leaked to hacking groups in North Korea and Russia.[43]

As the value of corporate assets on the cloud (and thereby at risk) increases with further digitalisation and deployment of 5G and IoT, stronger security solutions are needed. The cost of cybercrime (from predominantly commercial espionage) could reach a million employment

---

[41] CSIS, The Economic Impact of Cybercrime and Cyber Espionage, July 2013

[42] Cazes, Verick, Al Hussami, Diverging trends in unemployment in the United States and Europe: Evidence from Okun's law and the global financial crisis, ILO Employment Working Paper 106, 2011

[43] Shane, Perlroth, Sanger, Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core, New York Times, November 12, 2017, accessed at: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

opportunities lost by 2025.[44] By the consequence of same logic, the number of incidents should rise more than proportionally, unless the effectiveness of cybersecurity protection outsmarts the incidents (which is yet to happen since the history of computing began) that counteract this effect.

Lack of viable policy options

IN THE CURRENT ECONOMIC AND STRATEGIC environment, it is inevitable that the risks of cyber espionage also carry an economic and commercial impact, and that Europe is inarguably exposed.

The security environment of the European private sector is far from adequate, suffering from poor protection of business confidentiality, and network resilience. The EU is revising its network and service security as it is amending its telecom legislation into the Electronic Communication Code in preparation for 5G deployment.[45] Moreover, the NIS directive of 2016 calls on the EU Member States to ensure that operators of "essential services" take appropriate and proportionate measures to manage the risk of cyber hacking – yet, attacks on business data confidentiality has not warranted any effective policy initiatives yet.

China's strategic emerging sectors

- Integrated circuits (ICs) and software
- New-generation networks (internet, digital TV and mobile networks)
- Advanced computing (grid-based and peta/teraflop computer systems)
- Biomedicine, genome research as well as traditional Chinese medicine
- Spatial applications combining 5G and satellite application (such as meteorological, environmental and geolocations)
- Civil aircraft and advanced engines
- AI, 5G and wearable devices
- New materials needed in IT, biotechnology and aerospace industries
- Electric and hybrid vehicles

Source: The 12th Five-Year Guideline for National Economic and Social Development for 2011-2016; The 13th Five-Year Guideline for National Economic and Social Development for 2016-2020.

However, mitigating cyber espionage threats – through policy, technology or awareness – will take many years. Especially attacks involving social engineering (which exploits the human judgement) will take considerable efforts, as "cyber hygiene" requires security by design, awareness and

[44] Based on supra 43; supra 44; CEPS, Employment 2025: How multiple transitions will affect the European labour market (NEUJOBS)

[45] European Commission, Directive Establishing the European Electronic Communications Code, COM(2016) 590 final/2, 2016/0288(COD), recast SWD(2016) 313 final

changes in behaviour throughout the entire business organisation.[46] But even in the most secure and resilient environment, threats can only be mitigated to a point. Like with all forms of crime, it is in the very nature of cyber threats that the assailants are always going to be two steps ahead of the targets for ingenuity, while defences are reactive and deployed once new techniques are detected. Even the most secure firewalls and encryptions can be hacked with some persistence, as long as the target is valuable enough.

The EU countries are still in the process of building up national emergency response teams (CERTs) in charge of critical infrastructure and establishing a better functioning network of incident response teams (CSIRTs). Arguably, Europe has not fully developed its capabilities for active cyber defence (ACD), to take effective and proactive measures in anticipation ahead of attacks to mitigate them. Nor are there yet a widespread deployment of cyber forensics tools that are critical for securing evidence for attribution.

Even if clear-cut attribution of government-sponsored commercial espionage could be proven, commercial entities will not make such evidence public due to the retaliation it would unleash. Moreover, presenting such evidence would be futile as espionage is not an infraction of international law; and in any case, any threat of legal sanctions is not credible due to the immunity of sovereigns. Neither are there any international legal norms against cyber espionage. Europol concurs that commercial cyber espionage is an attack vector that cannot be addressed under national criminal law, the EU directives nor the Convention on Cybercrime under the Council of Europe.[47] China – the government-sponsor mentioned in many incidents – resolutely refuses to acknowledge any attribution despite a "plethora of evidence",[48] without which no EU jurisdiction is in a position to name and prosecute individual Chinese government officials, as in the case of the US Department of Justice indictment of five PLA officers.[49]

However, even without any attribution or legal remedies, a détente (at least on the surface) could in theory be achieved by diplomatic means – a kind of Non-Proliferation Treaty for cyber espionage. The China-US cybersecurity agreement, signed by the Presidents Xi and Obama in September 2015, the signatories agreed not to engage in commercial cyber espionage against each other. The effectiveness of agreement is heavily disputed, with some experts reporting that the number of incidents is waning, while others claim the opposite as there are few means of detection, providing incentives to cheat on the agreement.

In any case, the efficacy of diplomatic cyber treaties is mere academics in the case of Europe, as the counterparts have no incentives to sign them. Discounting President Putin's PR follies with the Trump administration,[50] it is not ultimately Russia's interest to enter into a truce, as cyber tools are relatively more important to Russia's strategic arsenal than to its European adversaries.

---

[46] Business Europe, Position Paper, The Proposal for a Cyber Act, November 23, 2017, accessed at: https://www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2017-11-23_pp_cyber-security_act.pdf

[47] Europol, Internet Organised Crime Threat Assessment (IOCTA), 2017, accessed at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

[48] Harold, Scott W., Martin C. Libicki and Astrid Stuth Cevallos. Getting to Yes with China in Cyberspace, RAND Corporation, 2016, accessed at: https://www.rand.org/pubs/research_reports/RR1335.html

[49] Booz Allen Hamilton, Booz Allen Cyber4sight, Anticipatory, actionable intelligence to fight advanced cyber threats, accessed at: https://www.boozallen.com/s/product/cyber4sight.html;
Accenture, 2017 Cyber Threatscape Report, 2017; see also Fire Eye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016, accessed at: https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html

[50] de Haldevang, Putin claims Russia proposed a cyberwar treaty in 2015 but the Obama administration ignored them, Quartz, June 16, 2017, accessed at: https://qz.com/1007996/oliver-stone-putin-interview-vladimir-putin-says-russia-proposed-a-cyber-war-treaty-in-2015-but-obamas-administration-ignored-them/

China has offered to negotiate treaties with the core members of the Five Eyes alliance with considerable offensive capabilities of their own. Meanwhile approaches by Germany to negotiate a similar agreement has been shunned, and both Germany and the EU as a whole lacks credible deterrents or alliances that are able to engage in cyber warfare.

Conclusions
Closing the backdoor

AS THE CHINA AND THE US have closed their markets to each other in various degrees, Europe is the last market to be fully open to both. The situation is untenable to Europe, as it is increasingly locked out of the Chinese market, while it is short of diplomatic, strategic and technical solutions to put an end to commercial cyber espionage through its backdoor.

If the EU cannot keep its house safe from intruders exploiting backdoors, it will lock its front door. This means imposing checks and balances on the open economic exchange that takes place between the EU and China.

Firstly, a recently proposed EU legislation on product certification requirements will cover "the whole spectrum of security requirements" against attacks.[51] The justification for this legislation explicitly states the need for action against cyber espionage with "intent of providing competitive advantages to companies.[52]

Secondly, some EU Member States may introduce screening of equipment for government use, reflecting recent legislative developments in the US and China.[53] Some EU Member States may even extend their existing screening for government use to equipment for commercial markets.[54]

Thirdly, an economy-wide investment screening at an EU-level has been proposed in addition to the national competence,[55] with the protection of electronic communications, cybersecurity and critical infrastructure as factors for consideration on all levels of decision-making. In addition, individual Member States will strengthen their national investment screening to complement the EU legislation.

Finally, the EU has reached a political agreement on a "cyber diplomatic toolbox" of diplomatic responses to be deployed against adversaries, including sanctions. The conclusions stress also that responses can be without "requiring attribution to a state or a non-state actor.[56]

Some elected officials have stated on the record that EU investment screening will achieve "little while risking a trade war" with China.[57] Whether these measures actually secure European corporate data is almost secondary to the real objective – which is to create an opportunity cost for its adversaries that forces China to change its behaviour. This is consistent with Europe's playbook

---

[51] European Council, Council Conclusion on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building a strong cybersecurity for the EU – Council conclusions, November 20, 2017, 14435/17

[52] ibid. para 40;

[53] China Cyber Security Law, 2017; see also Selyukh, Palmer, U.S. law to restrict government purchases of Chinese IT equipment, Reuters, March 2017, accessed at: http://uk.reuters.com/article/uk-usa-cybersecurity-espionage/u-s-law-to-restrict-government-purchases-of-chinese-it-equipment-idUKBRE92Q18T20130327

[54] See e.g. French Code Pénal, Art. 226-3

[55] European Commission, Regulation establishing a framework for screening foreign direct investments in to the European Union, COM(2017) 487 final

[56] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17, June 7, 2017

[57] Brunsden, J, EU plan to curb Chinese takeovers risks 'trade war', Financial Times, September 17, 2017

for economic statecraft that forced the US into the Privacy Shield, or its historical use of antidumping cases against China.

The lack of viable options is not an uncommon security and foreign policy dilemma for the EU. The Union remains foremost an economic union that must solve most of its problems using economic policy instruments, such as trade. However, the Single Market is already sufficiently open for trade and investments with Europe's counterparts, with only one option at its disposal – to limit access to the Single Market in order to create an economic leverage.
By Europe's moral imperative, it is China's strategic choices that pushed it to the point of no return – thus, it is also China's responsibility to de-escalate the situation if it wants to keep the EU markets open for its exporters.

European manufacturing base competes already head-to-head with the emerging economies, and the EU executives have shown preparedness to deploy trade defence instruments and punitive tariffs against various chemicals, steel, solar panels and failed an investigation on network equipment in pursuit of some leverage.

The economics of commercial cyber espionage make non-action a political improbability. The scale of the losses makes commercial cyber espionage an issue too critical to be ignored, while the targets are often "sacred" national champions like Airbus or in sectors like engineering, infrastructure, chemicals and steel. ▪

The cost of cybercrime (from predominantly commercial espionage) could reach a million employment opportunities lost by 2025.

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY