State sponsored cyber attacks
Introduction

There is a growing realisation that our digital society can be exploited and abused in ways that are inimical to our values. There is also an increased awareness that we are looking at highly sophisticated state-sponsored attacks aim primarily for economic advantage. The attackers are growing in skills, scale and determination.

There is no lack of reports or documents. This collection of facts is gathered from open sources in order to give the reader an overview of the current state of play regarding state-sponsored cyber espionage. The collection focuses on Chinese economic espionage hence does not claim to give a full picture of state sponsored cyber activities neither does it draw other conclusions than the sources cited have done.

It is clear that China runs an elaborate system to scout our technologies, acquire them by all conceivable means and convert them into competitive products – or military advantages. An industry, as the Swedish defense industry that spends 16% of their revenue on R&D, is a prime target for them and other adversaries.

Awareness is vital, as it is only with an increased alertness of the threats and the actors we can have an informed discussion and work together to secure the safety of our digital society.

Robert Limmergård
Secretary General
Content

Background 4
• Perceptions
• Development
• Effects

China’s rational 17
• Economic development is an issue of national security
• Not distinguishing between public and private targets
• Six examples

A more vulnerable situation 30
• 5G, Internet of Things and Industry 4.0

The legal situation 34
• New Chinese domestic legislation but no international regulation

The legal role models of enhanced trust 38
Perceptions
Citizens’ **perception** of cyber attacks from other countries – global figures

Cyberattacks from other countries #3 global top risk

Perception fairly similar across regions

**ISIS and climate change seen as among top threats around the world**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Europe</th>
<th>Asia-Pacific</th>
<th>Middle East</th>
<th>Africa</th>
<th>Latin America</th>
</tr>
</thead>
<tbody>
<tr>
<td>Islamic militant group known as ISIS</td>
<td>62%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global climate change</td>
<td>61%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyberattacks from other countries</td>
<td>51%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The condition of the global economy</td>
<td>51%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large number of refugees leaving countries such as Iraq and Syria</td>
<td>39%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.S. power and influence</td>
<td>35%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Russia’s power and influence</td>
<td>31%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>China’s power and influence</td>
<td>31%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Figures represent global medians across 38 countries. ISIS not asked in Turkey. U.S. power and influence not asked in U.S. and Russia’s power and influence not asked in Russia.

Source: Spring 2017 Global Attitudes Survey, Q17a-h.

**Major concerns by region show divergences in top threat assessment**

Regional medians saying ___ is a major threat to our country

<table>
<thead>
<tr>
<th>Threat</th>
<th>Europe</th>
<th>Asia-Pacific</th>
<th>Middle East</th>
<th>Africa</th>
<th>Latin America</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISIS</td>
<td>74%</td>
<td>62%</td>
<td>*</td>
<td>54%</td>
<td>40%</td>
</tr>
<tr>
<td>Global climate change</td>
<td>64%</td>
<td>61%</td>
<td>44%</td>
<td>58%</td>
<td>74%</td>
</tr>
<tr>
<td>Cyberattacks from other countries</td>
<td>54%</td>
<td>52%</td>
<td>40%</td>
<td>53%</td>
<td>54%</td>
</tr>
<tr>
<td>The condition of the global economy</td>
<td>37%</td>
<td>46%</td>
<td>59%</td>
<td>51%</td>
<td>61%</td>
</tr>
<tr>
<td>A large number of refugees leaving countries such as Iraq and Syria</td>
<td>41%</td>
<td>35%</td>
<td>48%</td>
<td>55%</td>
<td>31%</td>
</tr>
<tr>
<td>The United States’ power and influence</td>
<td>31%</td>
<td>35%</td>
<td>50%</td>
<td>37%</td>
<td>47%</td>
</tr>
<tr>
<td>Russia’s power and influence</td>
<td>41%</td>
<td>29%</td>
<td>35%</td>
<td>31%</td>
<td>23%</td>
</tr>
<tr>
<td>China’s power and influence</td>
<td>30%</td>
<td>47%</td>
<td>20%</td>
<td>32%</td>
<td>25%</td>
</tr>
</tbody>
</table>

* ISIS item only asked across four countries in the Middle East and North Africa. No median calculated. In these four countries, ISIS is the top threat.

Note: Bolded figures note the top concern in each region. Underlined figures note the second highest concern in each region.

Source: Spring 2017 Global Attitudes Survey, Q17a-h.
Small enterprises perception of cyber attacks

How would cyber-criminals, if at all, affect your business?

Potential effect on business of small and medium enterprises (SMEs) due to cybercrime in 2016
Global survey report
November, 2016

- “Steal customer data” (26.5%) and “Damage reputation” (19.7%) are the most common concerns in regard to cybercrime.
- A decreasing percentage of SMEs feel safe when thinking about cybercrime, with theft of customer data being the most concerning effect.
- Beside the theft of customer data, business disruption is a major effect of cybercrime, especially in Europe and in the US.
- Europe: Significantly fewer SMEs feel safe when thinking about cybercrime and incrementally more perceive reputation damage as a possible key effect.
Multinationals perception of cyber attacks

Cyber Espionage Tops the List as Most Serious Threat Concern to Global Businesses in 2017

• The research surveyed 2,402 enterprise IT decision makers across Europe and the U.S.

• 20% of global organizations rank cyber espionage as the most serious threat to their business, with a quarter (26%) struggling to keep up with the rapidly evolving threat landscape. In addition, one in five (20%) U.S. organizations have suffered a cyber espionage-related attack in the last year.

• Businesses in Italy (36%), France (24%), Germany (20%) and Netherlands (17%) topped the list for regions who fear cyber espionage the most.

• As more of our critical data is being moved online, nation states are now targeting businesses to obtain this data and businesses are struggling to keep up, which could also be placing critical infrastructure at risk.
Development
25% of all cyber-attacks are espionage

In 2016, 25% of all cyber-attacks across all sectors were motivated by espionage.


Sectors targeted by espionage motivated attacks: Manufacturing, Public Administration and Educational services.

FIG = Fun, Ideology, Grudge

In 2016, financial and espionage were still the top two motives combining to account for 93% of breaches.
94% of all cyber-attacks are espionage in the manufacturing sectors

Manufacturing sector includes all mechanical, physical, or chemical transformations of materials, substances, or components into new products.

When you make a product, there is always someone else who wants to make it better, or at least cheaper. A great way to make something cheaper is to let someone else pay for all of the R&D and then simply steal their intellectual property.

With that in mind, it will probably be of no surprise that cyber-espionage is by far the most predominant pattern associated with breaches.
Cyber-spies are highly active

90%

Ten years ago security researchers at the top vendors would have spent 90% of their time looking at criminal campaigns – big botnets, worms, emerging banking Trojans. Today the same researchers spend the same effort looking into targeted attacks, many of which are nation-state backed and aimed at either stealing secrets or at sabotage.
“Damage to interests in the telecom sector has an almost immediate adverse effect on national safety and security. Communication, including data communications, is vitally important to enable Dutch society to function unimpeded. The telecom networks are being targeted by foreign intelligence services (espionage). This makes telecom both a core interest and a vulnerability. The vulnerabilities in the telecommunication sector have direct repercussions on all other sectors.”

**Analysis of vulnerability to espionage**

- Categories of core interest
- Datasets and blueprints such as patents
- Position and strategies such as negotiating strategies
- Scientific innovations such as nano technology
- Soft and hard vulnerabilities
- Hack, tap and monitor people
- Interconnectivity, storage, linked storage, outsourced management, data processing, data warehousing
Chinese state-sponsored cyber operations – reactions in Washington

• In August 2017, President Trump launched an investigation into Chinese acts, policies, and practices related to technology transfer, intellectual property, and innovation.

• The U.S. Trade Representative (USTR) led the investigation under Section 301 of the Trade Act of 1974 that concluded that China, for over 10 years, has conducted and still supports cyber intrusions into U.S. companies to access their sensitive commercial information.

• The report acknowledged that China’s cyber activities represent a grave threat to U.S. competitiveness and the U.S. economy and that China’s government-directed cyber capabilities exist alongside an institutional framework that provides state-invested enterprises and national champions with privileged access to various forms of Chinese government support and information.

• The U.S. Intelligence Community judges that Chinese state-sponsored cyber operators continue to support Beijing’s strategic development goals, including its S&T advancement, military modernization, and economic development.
Effects
Estimated global cost of cyber crime and espionage

Total global cost of cyber crime and espionage

>600 BUSD

~1% of GDP
90% of cyber attacks impact a company’s intangibles

- The direct costs commonly associated with data breaches are far less significant than the “hidden” costs. In Deloitte’s scenarios, these account for less than 5% of the total business impact.

- The time horizon over which impact is felt is far more protracted than is often anticipated. In Deloitte’s scenarios, costs incurred during the initial triage stage of incident response account for less than 10% of the rippling impacts extending over a five-year period.

- Over 90% of cyberattack impact is likely to accrue in categories that are intangible. Given that these are less studied and more difficult to quantify, organizations can be caught especially unprepared for these “costs” in areas such as operational disruption, impact to brand and loss of intellectual property.
China’s rational
between Xi and US President Barack Obama, held during 7–8 June 2013, the issue of cyber security was put at the top of the bilateral agenda – albeit without Xi giving any ground by acknowledging China’s culpability.69 One month later, there was the first meeting of the new cyber-security working group within the framework of the annual US–China Strategic and Economic Dialogue.70 Xinhua, China’s official news agency, described the discussion as having gone well,71 but there was little evidence that the sides had made much progress. By that point rogue National Security Agency contractor Edward Snowden had begun to make revelations about the extent of cyber espionage carried out by the US and its Five Eyes allies (Australia, Canada, New Zealand and the United Kingdom). Snowden’s disclosures reinforced Chinese perceptions that the US was using its privileged position within the cyber domain to perpetuate American hegemony, and that Washington’s accusations against Beijing reflected double standards.72 In making its case against China’s statesponsored cyber industrial espionage, the US government sought to distinguish between conventional state-on-state spying for the purposes of national security – an activity that is not proscribed by international law – and the theft of intellectual property. The US argued that China had breached its treaty commitments as a member of the World Trade Organisation, specifically in connection with the Trade-Related Aspects of Intellectual Property Rights (TRIPS), which oblige governments to protect intellectual property.73 This interpretation of TRIPS was contentious in that, as Chinese experts on international law quickly pointed out, it was never conceived of as having an extraterritorial dimension.74 Moreover, Chinese security officials privately made clear that, for China, economic development was an issue of national security, since the CCP’s failure to achieve its economic goals might give rise to widespread social unrest, creating an existential threat to the regime.75 In effect, these officials were saying that cyber industrial espionage was a quasi-legal way to

“Failure to achieve economic goals might give rise to widespread social unrest, creating an existential regime threat to the regime”

In Chinese politics, economic development is an issue of national security

In Chinese politics, economic development is an issue of national security

“Failure to achieve economic goals might give rise to widespread social unrest, creating an existential regime threat to the regime”
China’s cyber security policies – not distinguishing between public and private targets

Amy Chang:

“China’s network security policies are motivated . . . by the Chinese Communist Party’s goal of maintaining its own governing power . . . [by ensuring] domestic stability, territorial integrity, modernization, and economic growth, while simultaneously preparing for the possibility of militarized cyber conflict in the future” p. 4

“No other country has been the target of EMCE complaints to the extent that China has, however. Furthermore, the United States has not specifically complained about other countries’ EMCE1 to the degree that it has cited China for such behavior. China, for its part, may view EMCE as a particularly attractive and legitimate form of espionage because of the closely intertwined nature of the Chinese state and economy. Thus, distinguishing espionage on public targets (legitimate) from espionage on private targets (illegitimate) accords more closely with the U.S. political-economic system than it does with China’s.” p. 60

1) EMCE, Economically Motivated Cyber Espionage
China’s cyber-espionage activities aimed at technology transfer to **regain historic levels**

After observing a downturn of activity in China, iDefense expects China’s cyber-espionage activities aimed at technology transfer to regain historic levels.

China’s 13th Five-Year Plan (FYP), which is now underway, may prompt the targeting of companies active in the areas of cyber-security, cloud computing and big data, new energy automobiles, high-performance computing, biomedical materials, repair and replacement of tissues and organs, **deep sea key technology and equipment**, and **smart grid technology and equipment**.

Historically, Chinese cyber-espionage operations have heavily targeted foreign technologies that overlap with FYP goals. Newly created after a military-wide restructuring, the Strategic Support Force of the People’s Liberation Army (PLA) is also tasked with supporting innovation and military development, including support through cyber-espionage means, and many FYP projects will likely reinforce this mission.
State sponsored espionage – a short cut to GDP growth

Total Factor Productivity gap between West and East Germany at the end of the Cold War would have been **6.3 percentage points larger** had the East not engaged in industrial espionage.

This paper, investigates the economic returns to industrial espionage by linking information from East Germany’s foreign intelligence service to sector-specific gaps in total factor productivity (TFP) between West and East Germany. It demonstrates that the economic returns to industrial espionage are primarily driven by relatively few high quality pieces of information and particularly strong in sectors that were closer to the West German technological frontier.

This paper presents the first systematic evaluation of the economic returns to state-sponsored industrial espionage. The Stasi archives and their rich information on industrial espionage. Findings show that the returns to industrial espionage were substantial, enabling East Germany’s economy, at least to some extent, to keep up with productivity growth in the West.

Arguably, few contemporary intelligence agencies have been able to make industrial espionage as effective a tool as the Stasi did during the Cold War. While, since then, the relative benefits of industrial espionage may have declined due to more integrated international markets and easier access to new ideas through legitimate channels, its costs have likely fallen even more in the wake of the digital revolution and the emergence of cyber-espionage as a new and comparatively cheap method of illicit technology transfer. Most developed countries nowadays therefore view industrial espionage as a severe and growing threat to their economies, making the topic as relevant today as it was at the height of the Cold War.

The processes through which newly acquired information is translated into productivity growth today may not differ much from the processes in place in East Germany at the time of the Cold War, especially in countries characterized by strong centralized governments such as China and Russia.
Six examples
Our research and observations indicate that the Communist Party of China (CPC) is tasking the Chinese People’s Liberation Army (PLA) to commit systematic cyber espionage and data theft against organizations around the world.

APT1 is believed to be the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (613989).

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries. The industries APT1 targets match industries that China has identified as strategic to their growth.

1) APT1 is one out of twenty specific Chinese group of Advanced Persistent Threat studied.
Example 2:

Operation Cloud Hopper – actor APT10 – highly likely to be a China-based threat actor

Who are the industrial targets?

PwC UK and BAE Systems assess it is highly likely that APT10 is a China-based threat actor with a focus on espionage and wide ranging information collection.

As a result of our analysis of APT10’s activities, we believe that it almost certainly benefits from significant staffing and logistical resources, which have increased over the last three years, with a significant step-change in 2016.

Espionage attacks associated with China-based threat actors, as noted above, have traditionally targeted organizations that are of strategic value to Chinese businesses and where intellectual property obtained from such attacks could facilitate domestic growth or advancement.
Example 3:

MSS, Boyusec and Huawei links established
Example 4:

Australia under attack, 2007-2011

The high-profile case of Chinese economic intelligence gathering has been widely reported in Australian media. The attempted merging of BHP Billiton and Rio Tinto, which would have created the largest iron ore exporter in the world, led to consternation in the Chinese mining industries.

The Chinese were anxious that the merger would create a monopoly that would be able to exert greater control over the pricing of minerals largely exported to China. Subsequently, both BHP’s and Rio Tinto’s computer networks were penetrated.

<table>
<thead>
<tr>
<th>Table 2: Australian cyberattacks reported in the media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Attributed to: China</td>
</tr>
<tr>
<td>September 2007</td>
</tr>
<tr>
<td>2007/2008</td>
</tr>
<tr>
<td>July 2009</td>
</tr>
<tr>
<td>July 2009</td>
</tr>
<tr>
<td>April 2010</td>
</tr>
<tr>
<td>April 2010</td>
</tr>
<tr>
<td>April 2010</td>
</tr>
<tr>
<td>May 2011</td>
</tr>
<tr>
<td>March 2013</td>
</tr>
<tr>
<td>Attributed to: Chinese Government/ intelligence</td>
</tr>
<tr>
<td>April 2010</td>
</tr>
<tr>
<td>September 2010</td>
</tr>
<tr>
<td>March 2011</td>
</tr>
</tbody>
</table>
by hackers from China, who were gathering information on the merger and on the advisory companies assisting the deal.

Not long afterwards, the Chinese state-backed company, Chinalco, became active as a blocking bidder for Rio Tinto. This led to the collapse of the merger and the loss to shareholders of potentially millions of dollars as a result.
Example 5:

Dispute along cold war lines led to collapse of UN cyber warfare talks

Thirteen years of negotiations at the United Nations aimed at restricting cyberwarfare collapsed in June (2017), it has emerged, due to an acrimonious dispute that pitted Russia, China and Cuba against western countries.

Negotiations aimed at forging an international legal framework governing cybersecurity began in 2004 including experts from 25 countries.

At previous sessions, officials accepted that the principles of international law should apply to cyberspace, including the UN charter itself. Article 51 of the charter states that nothing shall “impair the right of individual or collective self-defense” in the face of an armed attack.

But in June, diplomats at the UN abandoned any hope of making further progress, amid a row centered on the right to self-defense in the face of cyber-attacks.

Countries that oppose Article 51 “believe their states are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions”

Mike Schmitt, professor of international law at Exeter University and a former US air force lawyer, has been monitoring the UN GGE discussions. He said he feared a calculated decision has been made by Moscow and Beijing that the west has more to lose if there is no guaranteed right to retaliate against cyber-attacks.
Example 6:

China aiming for supremacy – building world’s biggest quantum research facility

China is building the world’s largest quantum research facility to develop a quantum computer and other “revolutionary” forms of technology that can be used by the military for code-breaking.

Pan Jianwei, China’s lead quantum scientist who was playing a key role in the project, told local officials at a briefing in May that technology developed in the facility would be of immediate use to the armed forces, according to Anhui Business Daily newspaper.

Another key mission of the laboratory is to build the nation’s first quantum computer that could break an encrypted message in seconds.

“Our plan is that by 2020, or maybe as soon as next year, to achieve ‘quantum supremacy’ with calculation power one million times to all existing computers around the world combined,” Pan was quoted as saying by Anhui Business Daily, which is run by the provincial government.

Construction work is expected to finish in 2 ½ years with a budget of 76 billion yuan (HK$91.6 billion).
The situation will become more vulnerable
New industrial applications in 5G increase the risk of economic espionage

5G will enhance existing and expand to new use cases and thus and to the risks of espionage

- Smart homes/buildings/cities
- Autonomous vehicles, object tracking
- Critical infrastructure protection & control, e.g. Smart Grid
- Remote control & process automation, e.g. aviation, robotics
- **Massive Internet of things**: Efficient, low cost communication with deep coverage
The legal situation
New Chinese foreign intelligence legislation

Required assistance to facilitate state-sponsored espionage – new in 2017

In addition to the power delegated to the intelligence agencies, the law mandates that all Chinese citizens and organizations in China (including governmental authorities, armed forces, political parties, social organisations, state-owned enterprises, private companies, and public institutions) shall cooperate with the Competent Authorities (intelligence agencies) when they are performing their duties by providing assistance.

Outside China, Chinese companies, whether state-owned or private – from national champions to acquired ex-foreign companies may face similar challenges from insider threats from Chinese nationals forced to facilitate state intelligence activities.

All relevant national departments shall, depending on their own functions and responsibilities, work closely with the agencies for State intelligence work.

Article 6
All state organs, armed forces, political parties, social organisations, enterprises, public institutions and citizens shall provide support and assistance to and cooperate with the State intelligence work, and keep secret the State intelligence work that they know.

Article 7
The State intelligence work shall be conducted according to the law, ensuring respect for and assurance of human rights and efforts to safeguard the legitimate rights and interests of citizens and organizations.

Article 8
The State protects individuals and organizations that provide support and assistance to the State intelligence work, and rewards those who have made great contributions.

CHAPTER II: FUNCTIONS AND POWERS OF AGENCIES FOR STATE INTELLIGENCE WORK

Article 9
Agencies for State intelligence work may make use of necessary methods, approaches and channels according to the law to carry out intelligence work within and outside of China, depending on their operational needs.

Article 10
Agencies for State intelligence work shall legally collect and process the relevant information about activities jeopardizing the national security and interests of the People's Republic of China that are conducted by any overseas agency, organization or individual itself, or by any other party under the instruction or assistance of such overseas agency, organization or individual, or by any domestic agency, organization or individual in collusion with an overseas agency, organization or individual.

Article 11
Any overseas agency, organization or individual that conducts any activity within the territory of China to harm the national security and interests of the People's Republic of China must be subject to legal liability. Agencies for State intelligence work shall provide intelligence information as a reference or basis to prevent, curb and punish such activity.

Article 12
Agencies for State intelligence work may build up bonds of cooperation with relevant individuals and organizations, and entrust them to perform relevant work.

Article 13
Relevant departments of the people's governments at all levels, enterprises, public institutions or other organizations and citizens shall give necessary assistance to the agencies for State intelligence work for their operations and keep them secret.

Article 14
Agencies for State intelligence work may, in light of their operational needs, adopt technical measures for investigation purpose after they have gone through strict approval procedures in accordance with relevant provisions of the State.
State sponsored economic espionage is not regulated by international law

“The current state of play leaves economic espionage relatively unregulated, which may explain why governments resort to other measures of unilateral nature instead, such as economic sanctions, or negotiating political commitments from states accused of engaging in economic espionage.”

Illustration of International and domestic law

Challenging economic espionage

<table>
<thead>
<tr>
<th>Option</th>
<th>Summary of findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>International (customary) law challenge by state</td>
<td>Espionage is per se not unlawful. Other principles, such as sovereignty, would have to be violated</td>
</tr>
<tr>
<td>Domestic court challenge by affected company</td>
<td>Attribution and evidence, claiming non-state immunity</td>
</tr>
<tr>
<td>Bilateral Investment Treaty, by affected company</td>
<td>Company would have to have an investment in the state, and show a link to the failed investment</td>
</tr>
<tr>
<td>WTO (TRIPS) challenge</td>
<td>Uncertain application, due to wording of provisions and geographical limitation of WTO commitments</td>
</tr>
<tr>
<td>Economic sanctions</td>
<td>Possible as a unilateral measure, however requires a form of national security test</td>
</tr>
<tr>
<td>Bilateral commitments</td>
<td>Lack of enforcement of commitments</td>
</tr>
</tbody>
</table>
The legal role models of enhanced trust in cyber security
The role models of enhanced ICT vendor trust

In order to ensure economic and societal benefits from 5G, IoT and Industry 4.0 countries can adopt in their domestic legislation essential mechanisms to screen for ICT vendors’ independence.

By comparing how the French and Australian regimes are constructed to limit espionage threat from ICT infrastructure, a number of generic legal features should be considered by legislators in other countries wishing to codify, implement, or modify similar legislation.

The Model in table 1 incorporates the identified strengths, as well as proposed remedies to the identified weaknesses of the respective French and Australian approach.

<table>
<thead>
<tr>
<th>Model Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal basis in the national legal order</strong></td>
</tr>
<tr>
<td><strong>Legal justification</strong></td>
</tr>
<tr>
<td><strong>Legal hierarchy</strong></td>
</tr>
<tr>
<td><strong>Autonomous assessments</strong></td>
</tr>
<tr>
<td><strong>Scope and Assessments</strong></td>
</tr>
<tr>
<td><strong>Scope: What should be covered by the law</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Mandatory Assessments</strong></td>
</tr>
<tr>
<td><strong>Authority and effects of assessments</strong></td>
</tr>
<tr>
<td><strong>Authority: Who should assess</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Effects of the assessment</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Sources:


12 China’s Cyber Power. IISS, 2016.  

13 Getting to Yes with China in Cyberspace, RAND Corporation, 2016.  
http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf


https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html


19 Enter the Cyber Dragon - Understanding Chinese intelligence agencies’ cyber capabilities, Australian Strategic Policy Institute (ASPI), 2013.  
https://www.files.ethz.ch/isn/165376/10_42_31_AM_SR50_chinese_cyber.pdf

20 Bowcott, Owen. 2017. Dispute along cold war lines led to collapse of UN cyberwarfare talks. The Guardian. 23 August.  


https://www.slideshare.net/qualcommwirelessevolution/designing-the-5g-unified-air-interface

https://www.qualcomm.com/documents/ihs-5g-economic-impact-study


24 French Penal Code, Article 226-4 of the Code Pénal and article 4 of the decree no. 2009-834 of 7 July 2009.  
https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations
