JONES DAY®

JANUARY 2014

EUROPE PROPOSES NEW LAWS AND REGULATIONS ON CYBERSECURITY

EUROPE PROPOSES NEW LAWS AND REGULATIONS ON CYBERSECURITY

Government-sponsored cyber thieves, criminals, and political activists are regularly attacking websites, networks, computers, and email accounts of governments, corporations, and individuals worldwide. Across Europe, hackers have targeted NATO, government agencies, and corporate networks for years. In Belgium, the Czech Republic, Ireland, Portugal, and Romania, hackers attacked government computers with malware called "MiniDuke" that has also hit individuals in Germany, the UK, and elsewhere. In Germany, a cyber attack knocked a power utility company's internet communications system offline for nearly a week. In the UK, the National Audit Office estimated in February 2013 that cyber crime cost the country between £18 billion and £27 billion in one year. Governments are beginning to take countermeasures, and regulatory trends are emerging.

In the following an overview shall be provided about the current legislative developments in the area of cybersecurity on the European level and in Germany, the United Kingdom, the Benelux countries, France, Italy, and Spain.

European Level

In February 2013, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy published a strategy for "An Open, Safe and Secure Cyberspace" (the "Strategy") and a proposed Cybersecurity Directive. In addition, the Irish EU presidency announced that the mandate for the European Network and Information Security Agency ("ENISA") would be renewed for seven years per an agreement between the EU Council, the European Parliament, and the European Commission.

This comes on top of existing EU legislation covering cyber incidents only sporadically. This includes in particular:

- The E-Privacy Directive (2002/58/EC) already requires electronic communications providers to appropriately manage risks to their networks and report significant breaches of security or network integrity.
- The European Critical Infrastructures Directive (2008/114/EC) obliges critical infrastructure operators to designate a security liaison officer and to develop security plans including risk analysis and countermeasures for service interruption or infrastructure destruction.
- The Data Protection Directive (95/46/EC) obliges data controllers to implement appropriate technical and organizational measures to protect personal data. A new General Data Protection Regulation has been proposed and is currently debated before the European Parliament. It includes new obligations, such as the obligation to appoint a data representative in the EU and to notify personal data breaches. However, under the current legal framework, there is no general obligation to report personal data breaches to any supervisory authorities.

The Strategy proposes to establish common minimum requirements for network and information security among the Member States;set up coordinated prevention, detection, mitigation, and response mechanisms; and improve the preparedness and engagement of the private sector. The Strategy seeks to stimulate demand for highly secure ICT products and to certify these products by establishing a platform to identify good cybersecurity and by developing security standards in the area of cloud computing.

The proposed Cybersecurity Directive provides for establishing Computer Emergency Response Teams ("CERTs") in each Member State and obliges Member States to adopt their own network and information security ("NIS") strategy. The Directive includes requirements for cooperation and information exchange between the Commission and the Member States; these are especially relevant for market operators, including social networks, cloud computing service providers, and public administrations.

The Cybersecurity Directive requires Member States to create a "National NIS strategy" to define the strategic objectives, policies, and regulatory measures to achieve a high level of NIS in Member States.[1] To translate these strategic goals into actions, such as risk and incident analysis, governance frameworks, education, awareness training, and R&D plans, Member States must create national competent authorities on the security of network and information systems with the technical, financial, and human resources to monitor application of the Cybersecurity Directive and inform Member States of any incident. Additionally, Member States must set up a CERT for handling incidents and risks according to a predefined process.[2]

As cybersecurity issues are typically international, the Cybersecurity Directive promotes cooperation mechanisms between the Commission and national authorities. These must comply with minimum requirements in the Cybersecurity Directive, such as risk assessment plans for potential incidents; general measures on preparedness, response, and recovery; a strategy for sharing between the public and private sector; and a roadmap for NIS exercise, training, and awareness programs. The goal is to build a cooperation network in order to circulate early warnings on risks and incidents, coordinate responses on incidents, exchange information and best practices securely, publish nonconfidential information, and further discuss issues such as national NIS strategies, national NIS cooperation plans, and the role of CERTs.

Article 14 of the Cybersecurity Directive requires public administrations and market operators[3] to take "appropriate technical and organizational measures to manage the risks

posed to the security of the networks and information systems they use and control in their operations." The Article 14 also requires Member States to ensure that public administration and market operators notify competent authorities of all incidents having a significant impact on the security of the core services they provide. The competent national authority then may decide to inform the public, or require the public administrations or market operators to do so, when it deems that such disclosure is in the public interest. These requirements of Article 14 apply to all market operators that provide services within the European Union, not just to market operators that reside in the European Union.

Under Article 15, Member States must investigate all cases of noncompliance by public administrations or market operators. Moreover, they must ensure the competent authorities have the power to require market operators and public administrations to provide information to assess the security of their networks and information systems, undergo a security audit carried out by a qualified independent body or national authority, and provide the results to the competent authority. Article 17 provides for "effective, proportionate and dissuasive" sanctions for noncompliance, and Article 18 stipulates an 18-month transposition period for the Cybersecurity Directive to become binding in the national law of each Member State after adoption.

Whereas the U.S. approach to regulation focuses mainly on critical infrastructure, the Cybersecurity Directive extends regulation to include key internet companies (as "information service providers"). This will result in increased administrative burdens for affected companies that must also comply with any new U.S. and EU cybersecurity requirements.

Further, the proposed introduction of national competent authorities might lead to conflicts between the intelligence services and prosecution authorities. Moreover, the relationship of the incident notification obligation in the Cybersecurity Directive and the breach notification requirements for personal data in the proposed General Data Protection Regulation would need further clarification. Finally, it is unclear which cybersecurity standards are relevant for companies until the Cybersecurity Directive takes effect under national laws. Companies should follow the developments on an EU level closely, along with activities of their Member States and voluntary commitments by industry.

Germany

Germany started as early as 2005 to establish plans for protecting information systems,[4] followed by a strategy plan focusing on critical infrastructure,[5] and modifications of the legislation to the competence for the Federal Office for Information Security[6] in 2009.[7] The BSI, in cooperation with the Federal Association for Information Technology, Telecommunications and New Media,[8] also launched a voluntary program called "Alliance for Cybersecurity"[9] to inform and report on cyber incidents. The Alliance's goal is to provide current and valid information in the area of cybersecurity nationwide, and to advise stakeholders to help prepare for cyber incidents. The program is open for stakeholders such as companies (e.g., Deutsche Telekom AG, Sourcefire Germany GmbH, TÜV Informationstechnik GmbH, McAfee, and Avira), authorities, and research institutions (e.g., Fraunhofer FKIE, Institut für Internet-Sicherheit).

In February 2011, Germany's Federal Ministry of the Interior issued a "Cybersecurity Strategy for Germany," an important initiative aimed at uniting organizations of all sizes to pool information on cybersecurity techniques. The Strategy also sought to maintain cooperation within the Federal Government, and between the public and private sectors. A National Cybersecurity Council and National Center for Cyber Defense were created to inform the public about, and issue early warnings on, cyber attacks.[10]

Notwithstanding the creation and implementation of this Cybersecurity Strategy, German companies continue to be hacked. In early September, Vodafone Germany reported data for more than two million of its 36 million German users was stolen—including names, addresses, bank codes, and account numbers. Although it is unlikely the data would allow direct bank account access, the risk of successful phishing efforts to obtain real account information is high based on the type of data stolen.[11] In this case, a suspect who had insider knowledge was identified, and charges were filed quickly.[12] This situation underscores the importance of effective public–private cooperation toward cybersecurity practices.

On March 5, German Interior Minister Hans-Peter Friedrich proposed an IT Security Act that would impose certain minimum IT security standards on operators of critical infrastructure and telecommunications and information society service providers. Under the proposed legislation, such firms would be required to do the following:

- Within two years, implement appropriate organizational and technical safeguards and other measures—in accordance with state-of-the-art technology—to protect IT systems, components, and processes essential for the functioning of critical infrastructure. There would be some room for self-regulation, as industry and associations could develop sector-specific standards to comply with the proposed minimum IT security standards. These could then be rubber-stamped by the regulator.
- Regularly (but at least every two years) carry out security audits and provide an overview of any security defects discovered through such audits to the German BSI.
- Inform the BSI without undue delay of all serious impairment of their IT systems, components, and processes that could affect the proper functioning of critical infrastructure.

In addition, new obligations would be introduced into existing sector-specific laws requiring implementation of state-of-the-art technical measures to protect telecommunications and data processing systems against unauthorized access. The German Interior Ministry's draft cybersecurity law must first be approved by the German Government and then submitted to the German Parliament.

The proposal has drawn criticism for possibly creating over-regulation and an overlap in competencies, and for being too vague. In addition, it would impose a rather broad obligation upon companies to report disruptions on availability and incidents—including those that should not necessarily be regarded as suitable to trigger reporting obligations, given their insignificant impact. In light of those arguments and given the progress of the European legislation, deliberations on the proposal were on hold until after the recent federal elections.

However, with the revelations around the NSA scandal, the IT Security Act has resurfaced and gained attention again. German Interior Minister Friedrich is promoting strict IT security standards to be an integral part of the coalition agreement that is currently in negotiation between those parties (Christian and Social Democrats), which are likely to form the new German government. The Minister also intends to establish a European internet requiring internet providers to organize their data traffic using European networks only.[13]

Recently, the Federal Council (*Bundesrat*) of Germany proposed the introduction of a new criminal provision against the receiving (or fencing) of data into the German Criminal Code. This provision is supposed to target cyber crime, especially criminal activities regarding the trading of "digital identities" (e.g., credit card data or access data to online banking, email services, or social networks). Also, the new law contains provisions that would increase the range of punishments for spying and/or intercepting data if performed with an intention to damage or enrichment.[14]

From the above-described activities, it can be inferred that Germany appears headed toward mandatory regulations for numerous industries.

The United Kingdom

The UK Government has also made efforts to respond to the perceived threat. The 2010 National Security Strategy identified cyber attacks as a "Tier 1" threat and set aside £650 million over four years to develop a response. In November 2011, the Government issued the UK Cybersecurity Strategy, proposing:

- Working with companies that own and manage their Critical National Infrastructure ("CNI") to ensure key data and systems continue to be safe and resilient.
- Expanding Government advice to include a wider range of organizations whose resilience is a priority for the UK economy.
- Creating and building a dedicated and integrated civilian and military capability within the Ministry of Defense.
- Maintaining and strengthening the UK's ability to anticipate, prepare for, and disrupt hostile acts in cyberspace.
- Improving levels of professionalism in information assurance and cyber defense across the public and private sector, and establishing a scheme for certifying the competence of information assurance and cybersecurity professionals, and a scheme for certifying specialist training.
- Managing crucial skills and helping develop a community of "ethical hackers" in the UK to ensure networks are robustly protected.
- Raising awareness among the public and businesses of the threat, and actions they can take toward protection.

In 2011, the Government and private firms codesigned a Cybersecurity Information Sharing Partnership ("CISP"). CISP was intended to establish a new secure "collaboration environment," a joint industry/government-resourced "Fusion Cell" to provide analysis and support, and terms and conditions for information sharing and the necessary information support. In 2013, CISP was ready to launch an "interim capability" to enable private firms to sign up to begin testing the proposed procedures. In November, Scotland Yard approved that it would add 500 additional cyber crime officers to its specialist E-crimes unit.

The UK already obliges all data controllers to apply "appropriate technical and organizational measures" against unlawful processing, and, in cases of serious breach, the Information Commissioner can impose monetary penalties of up to £500,000. Financial services companies are subject to additional regulatory requirements, including the systems and controls rules of the FCA (Financial Conduct Authority) handbook. There have been significant fines for security breaches in the past.

The Benelux

The Benelux countries (The Netherlands, Belgium, and Luxembourg) are host to numerous multinational corporations and international organizations, including the European institutions and NATO in Brussels, European Courts in Luxembourg, as well as Europol and the International Courts in The Hague. Those countries are thus a regular target for cyber attacks.

On April 4, 2011, the three States signed a common declaration of intent on cybersecurity for exchanging information and expertise, sharing best practices, and improving public–private cooperation. After three joint conferences and running debates in the Benelux parliament, the adoption of the "action plan Senningen 2013-2016" on June 6, 2013 aims

at further supporting the Benelux cooperation, particularly in the fight against botnets, the exchange of good practices for public–private partnerships, and the cooperation between each country's CERTs. In parallel to this cooperation, each Benelux country is also pursuing its own national strategy.

In Belgium, cyber offenses have been criminalized since the Computer Crimes Act of November 2000. The Law of July 1, 2011, which partially implements Directive 2008/114, also ensures the cyber safety and protection of critical infrastructures—including the public electronic communications sector. This law forces critical infrastructure operators to indicate a point of contact and to develop a security plan to prevent, mitigate, and neutralize the risks of service interruption or infrastructure destruction. In December 2012, the federal government adopted a Cybersecurity Strategy program to identify cyber threats, improve cyber safety, and handle incidents. No specific legislation has been adopted so far, but further governmental discussions are ongoing on issues such as capacity building and standardization.

In The Netherlands, the government adopted its national cybersecurity strategy in February 2011[15] "to reinforce security of the digital society, in order to increase confidence in the use of ICT by citizens, the business community, and the government."[16] Concrete measures include adopting annual national risk assessments, intensifying investigation and prosecution of cyber crime, stimulating research and education, and developing a response capacity for ICT disruptions and cyber attacks.

As a result of such strategy, The Netherlands also launched a Centre for Cybersecurity (*het Nationaal Cybersecurity Centrum*) in January 2012, which hosts several public departments (including the Dutch CERT) as well as members of the security forces, and supports public–private cooperation especially for sensitive sectors (financial, telecommunications, energy, health care, transport, etc.). Its core tasks are to build up expertise and to provide advice, respond to threats and incidents, and reinforce crisis management processes. It publishes an annual report on cybersecurity issues in The Netherlands.[17]

A legislative proposal was introduced in July 2013 to force operators of strategic infrastructure (including electricity, gas, water, telecoms, transports, financial sector, and governmental entities) to notify ICT breaches to the *Nationaal Cybersecurity Centrum.* It is still subject to parliamentary debates.[18]

The Netherlands also adopted a specific cybersecurity strategy for defense in June 2012[19] built around six focal points: (i) adopting a comprehensive approach; (ii) strengthening the cyber defense of the Defence Organisation (defensive element); (iii) developing the military capability to conduct cyber operations (offensive element); (iv) strengthening the intelligence position in cyberspace (intelligence element); (v) strengthening the knowledge position and the innovative strength of the Defence Organisation in cyberspace, including the recruitment and retention of qualified personnel (adaptive and innovative elements); and (vi) intensifying cooperation, both nationally and internationally (cooperation element).

In Luxembourg, the Government established in July 2011 a CERT covering governmental entities and critical infrastructure operators, and a Cybersecurity Board Chambers to adopt a national strategic plan to fight cyber attacks.

On November 15, 2011, the Cybersecurity Board adopted the national cybersecurity strategy that identifies five priorities: (i) establish operational measures (preventive and reactive) to ensure infrastructure protection; (ii) improve the legal framework; (iii) develop national and international cooperation; (iv) inform, educate, and raise awareness about the risks; and (v) establish standards. As part of the implementation of such strategy, additional CERTs have been established for education and research networks (RESTENA-CSIRT), and municipal authorities or any other entity (CIRCL). The Grand-Ducal Regulation of March 12, 2012 implements Directive 2008/114 on critical infrastructures; only energy and transports are identified as critical.

France

In France, cybersecurity is a great concern and becoming a priority investment area for the government. They are considering tripling the Directorate-General of Armament's cybersecurity research and development budget in 2014. A mixed Commission (composed notably of representatives of relevant government agencies and the armed forces) drafted a white paper on Defense and National Security in 2008. The French President presented this paper, emphasizing the high priority of cybersecurity among French defense priorities.[20]

Following the white paper's publication, the French Network and Information Security Agency ("ANSSI") was set up in July 2009.[21] The ANSSI, an interdepartmental agency operating under the authority of the Prime Minister, would lead implementing a preventive policy consisting of:

- Detecting and reacting to cyber attacks;
- Preventing threats;
- Advising French public institutions and other essential entities; and
- Keeping the public informed about threats.

In February 2011, the ANSSI published a document relating to the national strategy for information systems defense and security, revealing four main French objectives:[22]

- Become a cyber defense world power;
- Safeguard France's ability to make decisions through the protection of information related to its sovereignty;
- Strengthen the cybersecurity of critical national infrastructures; and
- Ensure security in the cyberspace.

That year, the priorities conferred to ANSSI were extended to encompass drafting and implementation of proposals relating to the protection of the State's information systems, the coordination of governmental actions, and the grant of authorizations regarding security mechanisms that protect information protected by national defense secrecy.[23]

Also in 2011, the French Government created the Cyber Defense General Officer position within the Ministry of Defense. This Officer will head a committee guaranteeing information system protection via additional protection against cybersecurity-related risks (e.g., the Officer would be in charge, in case of cybersecurity attacks, of disconnecting a network and quickly resetting the system). The Cyber Defense General Officer is responsible for crisis management and collaborates with the ANSSI.

On April 29, 2013, a new white paper was published regarding defense and national security.[24] It grants ANSSI the ability to give instructions to "operators of vital importance ("OVI")," e.g., all the entities—public or private—essential for the State. At present, the OVI do not have the obligation to file declarations relating to cyber attacks they have encountered. However, a bill is currently being discussed that would provide for such an obligation, enabling the ANSSI to create an inventory of cyber attacks.

Italy

The CNAIPIC (National Anti-Crime Computer Centre for Critical Infrastructure Protection—"*Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*") is the public body and branch of the Italian police corps, operative since 2005, responsible for the cybersecurity of infrastructures operating in particular sectors, such as health care, transport, telecommunications, and energy. The CNAIPIC center is active 24/7 and comprises two departments: operational and technical. Its purpose is to intervene to prevent and fight cyber attacks, cyber crime, and industrial espionage.

On January 24, 2013, the Italian Government issued additional measures under Presidential Decree No. 67251, containing updated guidelines for the safeguard of the cybernetics and national cybersecurity, with a view of coordinating all national and international initiatives (the "Decree").

The goal of the Decree is to identify entities involved in national cybersecurity and their tasks. The organizational structure defined by the Decree includes three different levels. First, the Decree sets forth the need to adopt a national plan for Italian cyberspace security. Such plan defines the relevant strategic guidelines to follow at a national level, and it will be adopted by the Italian Chairman of the Ministries' Council upon proposal of the Interdepartmental Committee for the Security of the Republic (*Comitato Interministeriale per la Sicurezza della Repbblica*, "CISR").

Further, the Decree identifies CISR as the entity that shall: (i) implement the national plan for cyberspace security; (ii) plan the detailed activities required to achieve this aim; and (iii) promote collaboration among institutional bodies and private market players operating in the national cybersecurity field. The CISR is assisted in achieving these tasks by various Italian intelligence public entities, including the Department of Security Information (*Dipartimento delle informazioni per la sicurezza*, "DIS"), the Agency for the Internal Information and Security (*Agenzia informazioni e sicurezza interna*), and the Agency for the External Information and Security (*Agenzia informazioni e sicurezza esterna*).

The third level is aimed at handling cyber risks or incidents. In particular, the Cybersecurity Team (*Nucleo per la sicurezza cibernetica*) is entrusted with powers to plan and coordinate the response to cyber attacks and restore the networks and systems functionality. This team is also responsible for interacting with correspondent bodies appointed by other nations or international organizations, such as the European Union, NATO, and the UN, in the field of cybersecurity, in order to create a uniform and efficient response to cyber attacks.

The actual performance of the responses planned by the Cybersecurity Team is carried out by the Interdepartmental Board of Cybernetic Crisis (*Tavolo Interministeriale di Crisi Cibernetica*) and, as far as network and technical aspects are concerned, by the national Computer Emergency Response Team. Additionally, the Decree also provides that the Italian private market players (i.e., those supplying information services and the operators of critical infrastructures, both at national and European levels), must, *inter alia*, notify the Cybersecurity Team of all relevant violations of their networks and adopt specific "best practices" to achieve cybersecurity. The Decree provides for the above general legal framework for national cybersecurity in Italy; however, the necessary implementing laws and regulations shall be enacted in a second stage. This includes the national plan for cyberspace security, for which the Decree did not set a deadline for approval.

Spain

Currently in Spain, cybersecurity is established as a priority national security objective that is necessary to guarantee

the development of strategic economic sectors. As a result of this objective, various measures have been adopted in 2013 aimed at ensuring a general legal and institutional framework for cybersecurity matters.

On February 15, the government approved the Digital Agenda for Spain as the reference framework for creating a roadmap to establish Spain's strategy for achieving the objectives of the Digital Agenda for Europe. The approved Agenda sets objectives and action plans to be adopted regarding, among others, matters related to cybersecurity in order to create a reference framework in this area. One such plan is the recently approved "Trust Plan in the Digital Field," which establishes, as one of its main concepts, the implementation of European regulations on cybersecurity, including the Policy for the Networking and Information Security, the Regulations for Electronic Identity and Trust Services, and the Regulations for Protection of Personal Data.

Subsequently, on May 31, the Council of Ministers approved the 2013 National Security Strategy that conceives national security in a more comprehensive and global manner than in previous strategies,[25] and includes and extends the traditional concept of national security (which was restricted to defense and public safety) to new parties of the private sector and to new threats, including cyber threats. Among others, the main objectives of the 2013 Strategy can be summarized as:

- Creating a flexible institutional system to develop the coordinated action of the existing instruments and organizations in the security. With regard to cybersecurity, INTECO will be the central body that will manage and oversee the development of the measures to be adopted within the framework of the plans and strategies referenced in this document in matters of Spanish cybersecurity.
- The development of general rules applicable to the new concept of national security as defined in the 2013 Strategy are applicable to all sectors.
- To date, Spain does not have rules applicable to public and private sectors. Royal Decree 3/2010 of January 8, which regulates the National Security Framework in the Electronic Administration sector, only covers the Public Administration sector, excluding other critical infrastructures, companies, and citizens.
- In addition, it does not have integrated rules for such matters. The late recognition of the strategic importance of having a secure cyberspace has caused, among other things, that fully developed General National Cybersecurity rules have not yet been created. Also, aspects directly related to cybersecurity are regulated through different sectoral instruments. Therefore, among others, the Law 15/99 of December 13 of Protection of Personal Data and General Telecommunications Law, the Law of the Information Society and Electronic Commerce, and the Spanish Penal Code should be considered.[26]
- Promote actions to strengthen public–private collaboration and the security and strength of the networks, products, and services used by ICT employees in the industrial sector.
- Promote training of professionals in cybersecurity and motivate Spanish industry through a research and development plan
- Strengthen the implementation of a solid cybersecurity culture.
- Strengthen international collaboration.
- Promote efforts aimed at achieving an international cyberspace, which aligns the initiatives of all the countries that pursue a safe and reliable environment, safeguarding national interests.

Finally, on July 15, the Secretary of State for Telecommunications and the Information Society anticipated that the Government wanted, "before the year-end," a National Cybersecurity Strategy that allows: (i) identification in a "correct" manner of the potential threats; (ii) determination of how to respond to these threats; (iii) coordination between Administrations and companies for the adoption of measures; and (iv) definition of an organization that has "national reference centres," and an "increased coordination" among all companies, Administrations, and States.

In summary, compliance with the European Agenda, the transposition of the European regulations on cybersecurity, and the development and implementation of the Spanish National Cybersecurity Strategy that will eventually be passed will ensure that 2014 will bring about a single legal framework for cybersecurity in Spain.

Conclusion

All companies that own, operate, or provide technology for critical infrastructure facilities, and all companies that provide goods or services to such owners, operators, or vendors, should monitor legislative and regulatory developments in countries in which they or their customers do business for several reasons.

First, companies that own, operate, or provide technology for critical infrastructure facilities may be or become subject to legislative or regulatory requirements. Such companies will need to know whether they have any right to challenge this designation.

Second, companies that own, operate, or provide technology for critical infrastructure facilities asked to voluntarily cooperate and share information with a government need to know what "incentives" or legal protections are available. For example, they may be able to reduce potential liability for antitrust violations and/or their risk of loss of the information they provide.

Third, companies that support proprietary information, or products or services, to owners or operators of critical infrastructure facilities may need to reevaluate their contractual relationships. Companies may consider the possibility that those owners and operators may be called upon to provide information, including confidential information, to a government.

Fourth, companies may want to participate in governmental and regulatory actions in this field to ensure their interests are protected. Even companies that do not own, operate, or supply technology to critical infrastructure facilities, or provide other goods or services that are or become subject to cybersecurity legislation or regulation, must follow legislative and regulatory developments in this area. Practices required or voluntarily undertaken in response to such developments may effectively set new standards for the protection of information and trade secrets.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Robertson
London
+44.20.7089.5204
erobertson@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

Emmanuel G. Baud
Paris
+33.1.56.59.39.18
ebaud@jonesday.com

Edouard Fortunet
Paris
+33.1.56.59.38.34
efortunet@jonesday.com

Stefano Macchi di Cellere
Milan
+39.02.7645.4104
London
+44.20.7039.5959
smacchi@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com

Adapted with permission from Privacy & Security Law Report, Vol. 12, No. 44, November 11, 2013. Copyright 2013 The Bureau of National Affairs, Inc. (1.800.372.1033) www.bna.com.

ENDNOTES

1 *See* Art. 5 para 1 Cybersecurity Directive.
2 Open-ended catalogue of e.g. requirements such as high availability of communication services; confidentiality, integrity, and authenticity of information; location of CERT offices in secure sites.
3 The Cybersecurity Directive in Article 3 para 1 subpara 8 defines "market operator" as follows: (i) provider of information society services which enable the provision of other information society services, a nonexhaustive list of which is set out in Annex II; (ii) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a nonexhaustive list of which is set out in Annex II.
4 *Nationaler Plan zum Schutz der Informationsinfrastrukturen* (NPSI) (https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html).
5 *Umsetzungsplan KRITIS, Umsetzungsplan BUND* (https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html).
6 *Bundesamt für Sicherheit in der Informationstechnik* – BSI.
7 *Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes* (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.pdf?___blob=publicationFile).
8 *Bundesverband Infomationswirtschaft, Telekommunikation und neue Medien e.V.* (BITKOM).
9 *Allianz für Cyber-Sicherheit, see* https://www.allianz-fuer-cyber-sicherheit.de/ACS/DE/Home/Startseite.html.
10 http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/task-force.html.
11 *Hacker stiehlt Daten von zwei Millionen Vodafone-Kunden, Frankfurter Allgemeine Wirtschaft* (Sept. 12, 2013), http://www.faz.net/aktuell/wirtschaft/unternehmen/kriminalitaet-im-netz-hacker-stiehlt-daten-von-zwei-millionen-vodafone-kunden-12570370.html.
12 Friedrich Geiger and Archibald Preuschat, "Hacker Hits Vodafone in Germany," *Wall Street Journal* (Sept. 12, 2013), http://online.wsj.com/article/SB10001424127887324549004579070790469487248.html.
13 *Friedrich will IT-Sicherheitsgesetz durchsetzen,* Handelsblatt (Nov. 3, 2013), http://www.bundestag.de/presse/hib/2013_08/2013_426/02.html.
14 *Bundesrat fordert schärfere Gesetze gegen Datenhehlerei*, German Federal Parliament – Press Release, (August 19, 2013), http://www.bundestag.de/presse/hib/2013_08/2013_426/02.html
15 http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.
16 *Ibid.,* p. 4
17 The 2013 report is available at https://www.ncsc.nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-kwetsbaarheid-van-ict-onverminderd-hoog.html.
18 *See* http://www.internetconsultatie.nl/meldplicht_ict_inbreuken.
19 http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.
20 "The French Whitepaper on defence and national security 2008," Présidence de la République, June 2008, available at http://www.defense.gouv.fr/portail-defense/enjeux2/politique-de-defense/livre-blanc-2008.
21 Decree no 2009-834 creating the French Network and Information Security Agency (ANSSI), July 9, 2009.
22 "Information systems defence and security, France strategy," ANSSI.
23 Decree no 2011-170 (February 11, 2011), amending Decree no 2009-834 (July 9, 2009), creating the French Network and Information Security Agency (ANSSI).
24 "The French Whitepaper on defense and national security 2013" (April 29, 2013), Ministry of Defense, available at http://www.defense.gouv.fr/actualites/articles/livre-blanc-2013.
25 Security Strategy adopted in 2011.
26 In Spain, computer crimes are punishable under the Penal Code. These crimes have the same penalties as equivalent noncomputer crimes.