LOMBARD ODIER
LOMBARD ODIER DARIER HENTSCH

CIO Viewpoint
Special Report

Cybersecurity investment opportunities

Investment Solutions

9 March 2022

Russia's invasion of Ukraine has raised fears of a cyberwar with global consequences. We assess the threats and limiting factors behind any cyber aspect to the conflict. Beyond the immediate risks, we believe the war in Ukraine will drive further growth in cybersecurity, with a range of investment implications.

Stéphane Monier
Chief Investment Officer, Lombard Odier Private Bank

Key takeaways

- The conflict in Ukraine – long a focus of cyber attacks – has raised cyber risks worldwide
- Such attacks are not precision instruments and can have large unforeseen consequences – one reason that could deter nation-state attackers keen to avoid conflict escalation
- Cybersecurity has risen up country and company agendas. Its link to governance and reputational risk makes it an increasingly protected part of corporate spending, and we expect healthy growth here in coming years
- We are positive on the cybersecurity industry – and see growing implications for insurers

Ukraine's ongoing cyber struggles

Ukraine has long been a testing ground for cyber attacks, and Russia widely acknowledged as the biggest state-sponsored actor[1]. In June 2021, a NATO communiqué had already noted the risk of malicious cyber activities by Russia against its members. A confident cyberpower engaged in a military invasion has now raised digital alert levels worldwide.

Ukraine has been dealing with digital harassment for years, from the spread of disinformation via the internet, to vicious and costly malware – or malicious software – to disable infrastructure. Since 2014, when Russia annexed Crimea, attacks have risen. Government agencies, the electoral commission, banks, airports and power networks have all been targets. Earlier this year, hackers left the message: "Be afraid and expect the worst" on a number of Ukrainian websites, and hit others with 'distributed denial of service' (DDoS) attacks that overwhelmed them with traffic.

Such attacks have heightened risks for international companies and investors. In 2017, a vicious form of malware – a 'wiper virus' designed to wipe computer hard drives – called NotPetya attacked accounting software used by Ukrainian firms. The US and UK laid the blame at Russia's door. NotPetya spread to global companies including FedEx and Merck, causing an estimated USD10bn of damage. For investors, it highlighted the threat of collateral damage to firms worldwide, and the need for cybersecurity protection and resilience. An attack on one of Toyota's major suppliers on 28 February this year, which took place shortly after Japan announced sanctions on Russia, caused the firm to halt domestic auto production, and lead investors to fear wider supply chain vulnerability.

[1] 58% of nation-state cyber attacks come from Russia, according to a 2021 Microsoft Digital Defense Report

Weekly publication of Lombard Odier – Contacts: Investment Solutions, investment-solutions@lombardodier.com
Data as of 9 March 2022 unless otherwise stated.

Risks of cyber attack have risen

The risk of cyber operations being deployed in the current conflict is certainly elevated. Cyberattacks are comparatively cheap and easy to launch. In the public mind, they probably sit somewhere above sanctions, but below military or nuclear actions. Many would argue they are now just another facet of modern warfare. Even their threat spreads fear; perhaps more, some academics posit, than their direct impact. Although a widespread communications blackout in Ukraine might be difficult to orchestrate, even limited blocks on mobile networks could cause panic.

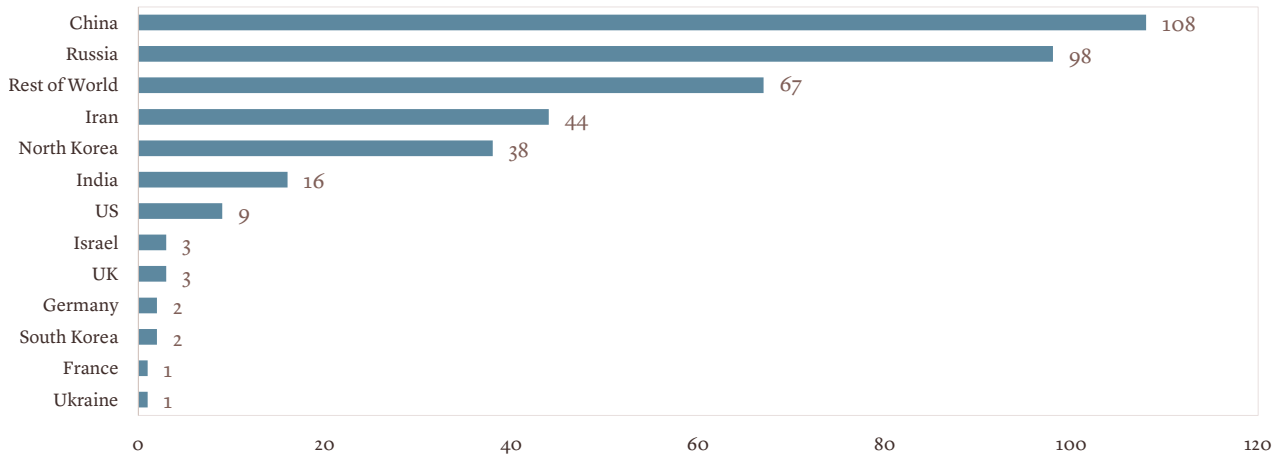
Thus far, however, there has not been the devastating cyberattack that many had feared. Ukraine has bolstered its cyber defences in recent years, and has now assembled a virtual army of cyber security professionals and hackers to attack Russia online: including taking down websites and pro-Russian content on social media, and reporting Russian troop locations. A separate activist hacking group called Anonymous has launched its own DDoS attacks on Russian media and government websites, and claims to have stolen files from Russia's defence ministry. Such unregulated guerrilla forces are one of the ways in which the conflict – and its associated risks – have already spilled way beyond the country's borders.

Threats for the West, companies and individuals

As the international response to Russia hardens, the risk of cyber retaliation has risen, perhaps on the instruments of the sanctions: Western government agencies, banks and financial infrastructure, or on strategic players in telecoms or technology. According to Reuters reports, both European and US regulators have warned banks to prepare for imminent cyber attacks.

Such attacks could have consequences beyond financial damage. NotPetya knocked out a radiation monitoring system at the defunct, but still contaminated, Chernobyl reactor. Previous attacks in Ukraine and Israel have targeted water, sewage and chlorine plants, with an

Significant cyber attacks since 2006
Attacker country of origin



Source: CSIS, Significant Cyber Incidents Timeline, GzeroMedia

attempt to contaminate water supplies. Hospitals, utilities, military command centres, Ukraine's 15 nuclear power stations – or indeed anything software-dependent– could potentially be vulnerable. On various occasions in recent years, hackers have taken control of parts of a Tesla car, opening up the possibility of hacking fleets of vehicles.

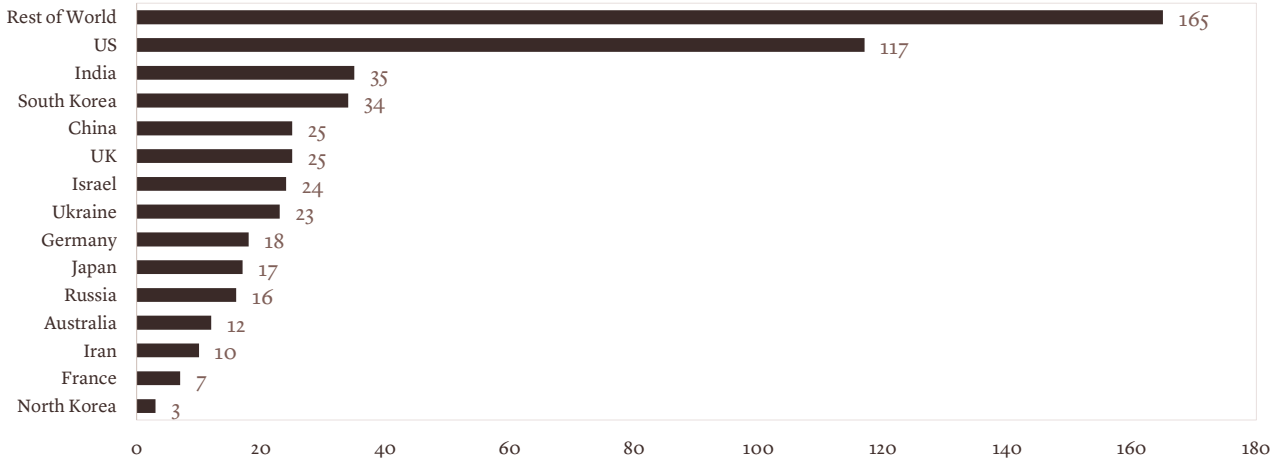
The latter goes to show that even in the most software-centric companies, vulnerabilities exist. Cyber attacks can target any industry or country, and the implications if cybersecurity risks are neglected can go well beyond data theft, to encompass reputational, operational, legal and compliance threats. One well-known case is that of Stuxnet, a malicious computer worm which was used to infect Siemens SCADA (Supervisory Control and Data Acquisition) and PLCs (programmable logic controller) systems to compromise the Iranian nuclear programme. Another was an attack on the British Airways app in 2018, where the personal data of almost 400,000 customers was compromised. The airline was fined GBP183mn for the breach, a figure that was later revised down to GBP20mn.

Cyber operations by the West?

Would the West potentially use cyber tactics against Russia? For years, many countries have used such methods to supplement traditional espionage and intelligence gathering. The New York Times claimed that in 2018, the US Cyber Command, part of the US military, attacked the Russian-based Internet Research Agency, to stop it spreading disinformation around the mid-term elections. But Western countries have been reluctant to use cyber powers to curb Russia's invasion of Ukraine. In part, this is because they would be contrary to measures and guidelines that the UN has been discussing to address international law and cyberspace. The West would be ill-placed to criticise Russia if it used tactics it had previously deplored. Besides, with more advanced digital integration and automation, many Western countries look more vulnerable than Russia to cyber attacks. In part also, there is the fear of unforeseen consequences triggering an escalation, and potentially drawing NATO members into an armed conflict with Russia.

Significant cyber attacks since 2006

Victim country of origin



Source: CSIS, Significant Cyber Incidents Timeline, GzeroMedia

Spill-over effects could be significant: one reason behind current restraint

The latter perhaps explains why we have not yet seen Russia deploy more digital weapons. Cyber attacks are not precision instruments, and the technology behind them is still in comparative infancy. NotPetya also ended up damaging Russian companies, including petroleum giant Rosneft. Ukrainian firms are a popular source of IT outsourcing services – the Ukrainian government estimates that over 100 Fortune 500 firms use such services, heightening the risk of wider contagion. Indeed, spill-over effects, or worse, the inadvertent loss of civilian life from a cyber attack, could see a rapid escalation from a localised to a more global conflict that both sides might be keen to avoid. There is also the growing possibility that the actions of private, autonomous hacktivists complicate the picture. The potential for such deadly miscalculations is one reason why financial markets remain so volatile.

100+

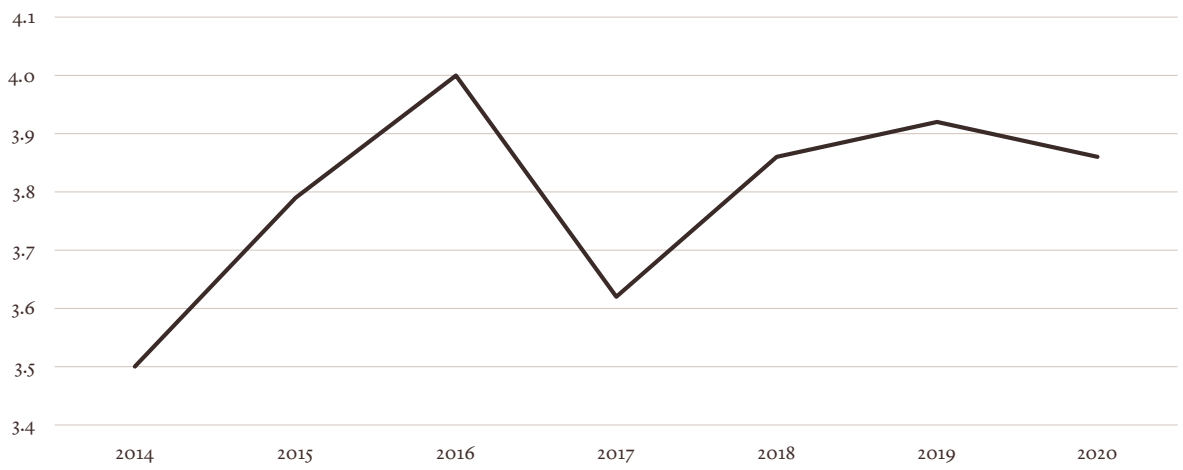
Fortune 500 firms use Ukrainian IT services

Investment implications across sectors

From a broader investment perspective, the war in Ukraine has certainly driven cybersecurity further up company and government agendas. This process had already started with the pandemic, when increased working from home broadened risks to data security. Many companies still lack adequate protection and data security measures: regular employee training and security software updates, measures such as two-factor authentication for online accounts, and cyber attack action plans.

Average cost of a data breach

USD mn



Source: Source: IBM Security, Cost of a Data Breach Report 2020

Industrial firms that provide automation and electrification products are exposed to the risk of hackers taking control of critical infrastructure. Many are already increasing capital expenditure on 'edge computing', which brings computing power and storage closer to the sources of data, reducing the risks associated with the transmission of sensitive data over the internet or cloud storage. Meanwhile, social media platforms face risks if they are not vigilant enough in removing false stories and inflammatory content.

Focus on cybersecurity firms

In light of the increased cyber risk arising from the Ukraine conflict, and a rise in remote working, we are positive on the cybersecurity industry. We consider the recent multiple compression – as rising nominal rates have weighed on high valuation stocks – as an interesting opportunity to build up positions. Cybersecurity is an increasingly critical and protected area of enterprise spend. Research firm Gartner estimates spending on IT security and risk management technology rose 12.4% to USD150.4bn in 2021 worldwide, and should grow at high single-digits until 2024.

12.4%

Growth in IT security and risk management technology spending in 2021

In the face of continually evolving risks, cybersecurity is also fast-evolving. The focus has shifted from the perimeter of the network to deeper within it, to endpoints (user devices, such as PCs, laptops, manufacturing equipment, or mobile phones), users, and applications. The 'attack surface' has opened up, complicating old concepts of security. The industry has responded by building more complete platforms, incorporating features that were previously offered on a standalone basis: firewalls that include cryptographic authentication of responses even from 'authorised' servers, and tools that continuously monitor networks for malicious activity. IT security companies play an increasingly critical role in business governance by securing enterprise and customer data, thereby mitigating reputational risks. Together, market and technology forces are driving the move to cloud-delivered deployments. We therefore see lower cyclicality in the industry moving forward, as it migrates from solutions tied to product cycles, towards software subscription models – and hence more reliable, recurring revenues.

Within cybersecurity firms, we prefer companies with complete security platforms over those with standalone products: the latter could see their solutions integrated into other platforms. Legacy network security vendors should maintain sticky relationships with customers but we expect growth to come from new cloud-based delivery of network security and from legacy players that are making rapid efforts to transition. We favour high quality names that benefit from secular growth via exposure to next-generation security, demonstrate an ability to execute, and exhibit strong cash flow generation.

Meanwhile, cyber insurance is also a very small but fast-growing part of the insurance market (currently responsible for just 0.4% of global property and casualty premiums, according to Swiss Re). Rising risks from increased remote working, and the heightened risk of cyber attack following Russia's invasion of Ukraine, could focus policymakers' minds on setting a clearer regulatory and legal framework going forward. That could pave the way for greater policy standardisation and market growth ahead.

0.4%

Cyber insurance's share of global property & casualty insurance premiums

Cyber attack methods and risks

Malware: 'Malicious software' is installed in a network when users click on a link or email attachment. It is among the most common forms of cyber attack, and comprises spyware, viruses, worms, Trojans and ransomware

Spyware: Collects information about the system or its users and passes it on to the attacker

Viruses: Like their biological counterparts, viruses attack the host by infecting applications and code across the system, replicating themselves as they go.

Worms: These programs are often installed via an email attachment, which sends a copy of itself to every user or contact in email lists. Worms do not attack the system but are often used to overload it

Trojans: Establish a back door into systems to create a vulnerability to attack. Trojans hide themselves inside legitimate programs.

Ransomware: Collects information but also denies access to the victim's data, including in some cases via encrypting it, and demands a ransom for its release.

Phishing: These attacks target users via fraudulent emails, phone calls or through social media, hoping to obtain their financial details, or to gain control of their device and use it to extract data

Distributed denial-of-Service (DDOS) Attacks: These attacks flood systems, servers or networks with information, effectively blocking them

Zero-day exploit: When cyber criminals exploit a vulnerability in well-known software or operating systems, to target organisations using them before a fix is found

Man-in-the-middle attack: Intercepts a two-way communication to obtain information, spy on the participants, or alter the outcome. End-to-end encrypted email and chat systems help prevent attacks

Cryptojacking: Where criminals compromise a company network or device and use it to mine cryptocurrencies without the organisation knowing.

Important information

This is a marketing communication issued by Bank Lombard Odier & Co Ltd (hereinafter "Lombard Odier"). It is not intended for distribution, publication, or use in any jurisdiction where such distribution, publication, or use would be unlawful, nor is it aimed at any person or entity to whom it would be unlawful to address such a marketing communication. This marketing communication is provided for information purposes only. It does not constitute an offer or a recommendation to subscribe, purchase, sell or hold any security or financial instrument. It contains the opinions of Lombard Odier, as at the date of issue. **These opinions and the information contained herein do not take into account an individual's specific circumstances, objectives, or needs. No representation is made that any investment or strategy is suitable or appropriate to individual circumstances or that any investment or strategy constitutes personalised investment advice to any investor.** Each investor must make his/her own independent decisions regarding any securities or financial instruments mentioned herein. Tax treatment depends on the individual circumstances of each person and may be subject to change in the future. Lombard Odier does not provide tax advice. Therefore, you must verify the above and all other information provided in the marketing communication or otherwise review it with your external tax advisors. Some investment products and services, including custody, may be subject to legal restrictions or may not be available worldwide on an unrestricted basis. The information and analysis contained herein are based on sources considered reliable. Lombard Odier uses its best effort to ensure the timeliness, accuracy, and comprehensiveness of the information contained in this marketing communication. Nevertheless, all information and opinions as well as the prices, market valuations and calculations indicated herein may change without notice.

Investments are subject to a variety of risks. Before entering into any transaction, an investor should consult his/her investment advisor and, where necessary, obtain independent professional advice in respect of risks, as well as any legal, regulatory, credit, tax, and accounting consequences. The investments mentioned in this marketing communication may carry risks that are difficult to quantify and integrate into an investment assessment. In general, products such as equities, bonds, securities lending, forex, or money market instruments bear risks, which are higher in the case of derivative, structured, and private equity products; these are aimed solely at investors who are able to understand their nature and characteristics and to bear their associated risks. On request, Lombard Odier will be pleased to provide investors with more detailed information concerning risks associated with given instruments. **Past performance is no guarantee of current or future returns, and the investor may receive back less than he/she invested**. The value of any investment in a currency other than the base currency of a portfolio is subject to the foreign exchange rates. Exchange rates may fluctuate and adversely affect the value of the investment when it is realised and converted back into the investor's base currency. The liquidity of an investment is subject to supply and demand. Some products may not have a well-established secondary market or in extreme market conditions may be difficult to value, resulting in price volatility and making it difficult to obtain a price to dispose of the asset. **This marketing communication is not issued by the organisational unit of the Bank Lombard Odier & Co Ltd responsible for the production of financial research**, as defined under the Swiss Bankers Association Directives on the Independence of Financial Research. Consequently, it is not prepared in accordance with the provisions of the referred Directives or any other legal requirements designed to promote the independence of the production of financial research. Opinions expressed in this marketing communication may differ from the opinions expressed by other divisions of Lombard Odier, including Bank Lombard Odier & Co Ltd's Research Department. Nevertheless, if opinions from financial analysts belonging to the Research Department are contained herein, such analysts attest that all of the opinions expressed accurately reflect their personal views about any given instruments. In order to ensure their independence, financial analysts are expressly prohibited from owning any securities that belong to the research universe they cover. Lombard Odier may hold positions in securities as referred to in this marketing communication for and on behalf of its clients and/or such securities may be included in the portfolios of investment funds as managed by Lombard Odier or affiliated Group companies. Lombard Odier recognises that conflicts of interest may exist as a consequence of the distribution of financial instruments or products issued and/or managed by entities belonging to the Lombard Odier Group. Lombard Odier has a Conflict of Interests policy to identify and manage such conflicts of interest.

European Union Members: This marketing communication has been approved for use by Lombard Odier (Europe) S.A. in Luxembourg and by each of its branches operating in the following territories: **Belgium**: Lombard Odier (Europe) S.A. Luxembourg • Belgium branch; **France**: Lombard Odier (Europe) S.A. • Succursale en France; **Italy**: Lombard Odier (Europe) S.A. • Italian Branch; **Spain**: Lombard Odier (Europe) S.A. • Sucursal en España. Lombard Odier (Europe) S.A. is a credit institution authorised and regulated by the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg. In addition, this marketing communication has also been approved for use by the following entity domiciled within the European Union: **Spain**: Lombard Odier Gestión (España) S.G.I.I.C., S.A.U., an investment management company authorised and regulated by the Comisión Nacional del Mercado de Valores (CNMV), Spain.

Hong Kong: This marketing communication has been approved for use by Lombard Odier (Hong Kong) Limited, a licensed entity regulated and supervised by the Securities and Futures Commission in Hong Kong for the general information of professional investors and other persons in accordance with the Securities and Futures Ordinance (Chapter 571) of the laws of Hong Kong.

Singapore: This marketing communication has been approved for use by Lombard Odier (Singapore) Ltd for the general information of accredited investors and other persons in accordance with the conditions specified in Sections 275 and 305 of the Securities and Futures Act (Chapter 289). Recipients in Singapore should contact Lombard Odier (Singapore) Ltd, an exempt financial adviser under the Financial Advisers Act (Chapter 110) and a merchant bank regulated and supervised by the Monetary Authority of Singapore, in respect of any matters arising from, or in connection with this marketing communication. The recipients of this marketing communication represent and warrant that they are accredited investors and other persons as defined in the Securities and Futures Act (Chapter 289). This advertisement has not been reviewed by the Monetary Authority of Singapore.
Panama: This marketing communication has been approved for use in Panamá by Lombard Odier (Panamá) Inc., an entity authorised and regulated by the Superintendencia del Mercado de Valores de Panamá. Licensed to operate as an Investment Adviser. Res. SMV No.528-2013.
Israel: This marketing communication has been approved for use in Israel by the Israel Representative Office of Bank Lombard Odier & Co Ltd, an entity not supervised by the Supervisor of Banks in the Bank of Israel, but by the Swiss Financial Market Supervisory Authority, which supervises the activities of Bank Lombard Odier & Co Ltd.
South Africa: This marketing communication has been approved for use in South Africa by the South Africa Representative Office of Bank Lombard Odier & Co Ltd, an authorised financial services provider Registration number 48505.
Switzerland: This marketing communication has been approved for use in Switzerland by Bank Lombard Odier & Co Ltd Geneva, a bank and securities firm authorised and regulated by the Swiss Financial Market Supervisory Authority (FINMA).
United Kingdom: This marketing communication has been approved for use in the United Kingdom by Lombard Odier (Europe) S.A. – UK Branch, a bank authorised and regulated by the Commission de Surveillance du Secteur Financier ("CSSF') in Luxembourg and authorised in the UK by the Prudential Regulation Authority ("PRA"). Subject to regulation by the Financial Conduct Authority ("FCA") and limited regulation by the Prudential Regulation Authority. Financial Services Firm Reference Number 597896. **Details about the extent of our authorisation and regulation by the Prudential Regulation Authority and regulation by the Financial Conduct Authority are available from us on request.**
United States: Neither this document nor any copy thereof may be sent to, taken into, or distributed in the United States of America, any of its territories or possessions or areas subject to its jurisdiction, or to or for the benefit of a United States Person. For this purpose, the term "United States Person" shall mean any citizen, national or resident of the United States of America, partnership organised or existing in any state, territory or possession of the United States of America, a corporation organised under the laws of the United States or of any state, territory or possession thereof, or any estate or trust that is subject to United States Federal income tax regardless of the source of its income.

Data protection: You may be receiving this communication because you have provided us with your contact details. If this is the case, note that we may process your personal data for direct marketing purposes. If you wish to object to this processing, please address your objection to the Group's Data Protection Officer: Bank Lombard Odier & Co Ltd, Group Data Protection Officer, 11, Rue de la Corraterie, 1204 Geneva, Switzerland. E-Mail: group-dataprotection@lombardodier.com. For more information on Lombard Odier's data protection policy, please refer to www.lombardodier.com/privacy-policy.
 Ref. LOCH/LOESA/LOASIA-MWNPR-en-092021.

SWITZERLAND

GENEVA
Bank Lombard Odier & Co Ltd[1]
Rue de la Corraterie 11 · 1204 Genève · Suisse
geneva@lombardodier.com
Lombard Odier Asset Management (Switzerland) SA
Avenue des Morgines 6 · 1213 Petit-Lancy · Suisse
Support-Client-LOIM@lombardodier.com
Management Company regulated by the FINMA.

FRIBOURG
Banque Lombard Odier & Cie SA · Bureau de Fribourg[1]
Rue de la Banque 3 · 1700 Fribourg · Suisse
fribourg@lombardodier.com

LAUSANNE
Bank Lombard Odier & Co Ltd[1]
Place St-François 11 · 1003 Lausanne · Suisse
lausanne@lombardodier.com

VEVEY
Banque Lombard Odier & Cie SA · Agence de Vevey[1]
Rue Jean-Jacques Rousseau 5 · 1800 Vevey · Suisse
vevey@lombardodier.com

ZURICH
Bank Lombard Odier & Co Ltd[1]
Utoschloss · Utoquai 29-31 · 8008 Zürich · Schweiz
zurich@lombardodier.com

EUROPE

BRUSSELS
Lombard Odier (Europe) S.A. Luxembourg · Belgium branch[2]
Avenue Louise 81 · Box 12 · 1050 Brussels · Belgium
brussels@lombardodier.com
Credit institution supervised in Belgium by the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA).

LONDON
Lombard Odier (Europe) S.A.· UK Branch[2]
Queensberry House · 3 Old Burlington Street · London W1S 3AB · United Kingdom
london@lombardodier.com
The Bank is authorised in the UK by the Prudential Regulation Authority (PRA). Subject to regulation by the Financial Conduct Authority (FCA) and limited regulation by the Prudential Regulation Authority. Financial Services Firm Reference Number 597896. Details about the extent of our authorisation and regulation by the Prudential Regulation Authority and regulation by the Financial Conduct Authority are available from us on request.
Lombard Odier Asset Management (Europe) Limited
Queensberry House · 3 Old Burlington Street · London W1S 3AB · United Kingdom
london@lombardodier.com
Investment firm authorised and regulated by the Financial Conduct Authority (FCA register No.515393).

LUXEMBOURG
Lombard Odier (Europe) S.A.
291, route d'Arlon · 1150 · Luxembourg · Luxembourg
luxembourg@lombardodier.com
Credit institution authorised and regulated by the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg.
Lombard Odier Funds (Europe) S.A.
291, route d'Arlon · 1150 · Luxembourg · Luxembourg
luxembourg@lombardodier.com

MADRID
Lombard Odier (Europe) S.A. · Sucursal en España[2]
Paseo de la Castellana 66 · 4ª Pl. · 28046 Madrid · España · madrid@lombardodier.com
Credit institution supervised in Spain, by the Banco de España and the Comisión Nacional del Mercado de Valores (CNMV).
Lombard Odier Gestión (España) S.G.I.I.C, S.A.U.
Paseo de la Castellana 66, 4ª Pl. · 28046 Madrid · España · madrid@lombardodier.com
Management Company supervised by the Comisión Nacional del Mercado de Valores (CNMV).

MILAN
Lombard Odier (Europe) S.A. · Succursale in Italia[2]
Via Santa Margherita 6 · 20121 Milano · Italia
milano-cp@lombardodier.com
Credit institution supervised in Italy by the Commissione Nazionale per le Società e la Borsa (CONSOB) and la Banca d'Italia.

PARIS
Lombard Odier (Europe) S.A. · Succursale en France[2]
8, rue Royale · 75008 Paris · France. RCS PARIS B 803 905 157 · paris@lombardodier.com
Credit institution supervised in France by the Autorité de contrôle prudentiel et de résolution (ACPR) and by the Autorité des Marchés Financiers (AMF) in respect of its investment services activities. Business permit No.23/12. Registered in Luxembourg · No.B169 907. Insurance intermediary authorised by the Commissariat aux Assurances (CAA) No.2014 CM002. The registration with the CAA can be verified at www.orias.fr.

AFRICA | AMERICAS | MIDDLE EAST

ABU-DHABI
Bank Lombard Odier & Co Ltd · Abu Dhabi Global Market Branch
Al Maryah Island · Abu Dhabi Global Market Square · Al Khatem Tower · 8th floor · P.O. Box 764646 · Abu Dhabi · UAE · abudhabi@lombardodier.com
Arranging Deals in Investments · Advising on Investment or Credit · Arranging Credit. Regulated by the ADGM Financial Services Regulatory Authority.

BERMUDA
Lombard Odier Trust (Bermuda) Limited
3rd Floor, Victoria Place · 31 Victoria Street · Hamilton HM 10 · Bermuda · bermuda@lombardodier.com
Licensed to conduct Trust, Investment and Corporate Service Provider Business by the Bermuda Monetary Authority.

BRASIL
Lombard Odier (Brasil) Consultoria de Valores Mobiliários Ltda.
Avenida 9 de Julho No. 3624, Torre DGN 360, 6° andar · Jardim Paulista · CEP 01406-000 · São Paulo · Brasil
sao.paulo.office@lombardodier.com
Supervised by the Comissão de Valores Mobiliários of Brazil.

DUBAI
Bank Lombard Odier & Co Ltd · Representative Office Dubai
Conrad Business Tower · 12th Floor · Sheikh Zayed Road · P.O. Box 212240 · Dubai · UAE
dubai@lombardodier.com
Under the supervisory authority of the Central Bank of the UAE.

ISRAEL
Israel Representative Office · Bank Lombard Odier & Co Ltd
Alrov Tower 11th floor · 46 Rothschild Blvd. · Tel Aviv 6688312 · Israel · telaviv@lombardodier.com
Not supervised by the Bank of Israel, but by Swiss Financial Market Supervisory Authority which supervises the activities of Bank Lombard Odier & Co Ltd.

JOHANNESBURG
South Africa Representative Office · Bank Lombard Odier & Co Ltd
4 Sandown Valley Crescent · Sandton · Johannesburg 2196 · South Africa · johannesburg@lombardodier.com
Authorised financial services provider Registration number 48505.

NASSAU
Lombard Odier & Cie (Bahamas) Limited
Lyford Cay House · Western Road · P.O. Box N-4938 · Nassau · Bahamas · nassau@lombardodier.com
Supervised by the Central Bank of the Bahamas and the Securities Commission of the Bahamas.

PANAMA
Lombard Odier & Cie (Bahamas) Limited · Representative Office in Panama
Oceania Business Plaza Torre 2000 · Oficina 38-D · Blvd. Pacifica · Urb. Punta Pacifica · Corregimiento de San Francisco · Panamá · panama@lombardodier.com
Supervised by the Central Bank of the Bahamas and the Superintendencia de Bancos de Panamá.
Lombard Odier (Panama) Inc.
Oceania Business Plaza Torre 2000 · Oficina 38-D · Blvd. Pacifica · Urb. Punta Pacifica · Corregimiento de San Francisco · Panamá · panama@lombardodier.com
Supervised by the Superintendencia del Mercado de valores de Panamá. Licensed to operate as an Investment Adviser. Res. SMV No.528-2013.

ASIA - PACIFIC

HONG KONG
Lombard Odier (Hong Kong) Limited
1601 Three Exchange Square · 8 Connaught Place · Central · Hong Kong · hongkong@lombardodier.com
A licensed entity regulated and supervised by the Securities and Futures Commission in Hong Kong.

SINGAPORE
Lombard Odier (Singapore) Ltd.
9 Raffles Place · Republic Plaza #46-02 · Singapore 048619 · singapore@lombardodier.com
A merchant bank regulated and supervised by the Monetary Authority of Singapore.

TOKYO
Lombard Odier Trust (Japan) Limited
Izumi Garden Tower 41F · 1-6-1 Roppongi, Minato-ku · Tokyo 106-6041 · Japan · tokyo@lombardodier.com
Regulated and supervised by the Financial Services Agency (FSA) in Japan. It holds a trust business license (FSA No.208) and is registered with Kanto Local Finance Bureau for Financial Instruments Business Operator (No.470).

[1] *Private bank and securities firm authorised and regulated by the Swiss Financial Market Supervisory Authority (FINMA).*

[2] *Branch of Lombard Odier (Europe) S.A., a credit institution based in Luxembourg, authorised and regulated by the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg.*