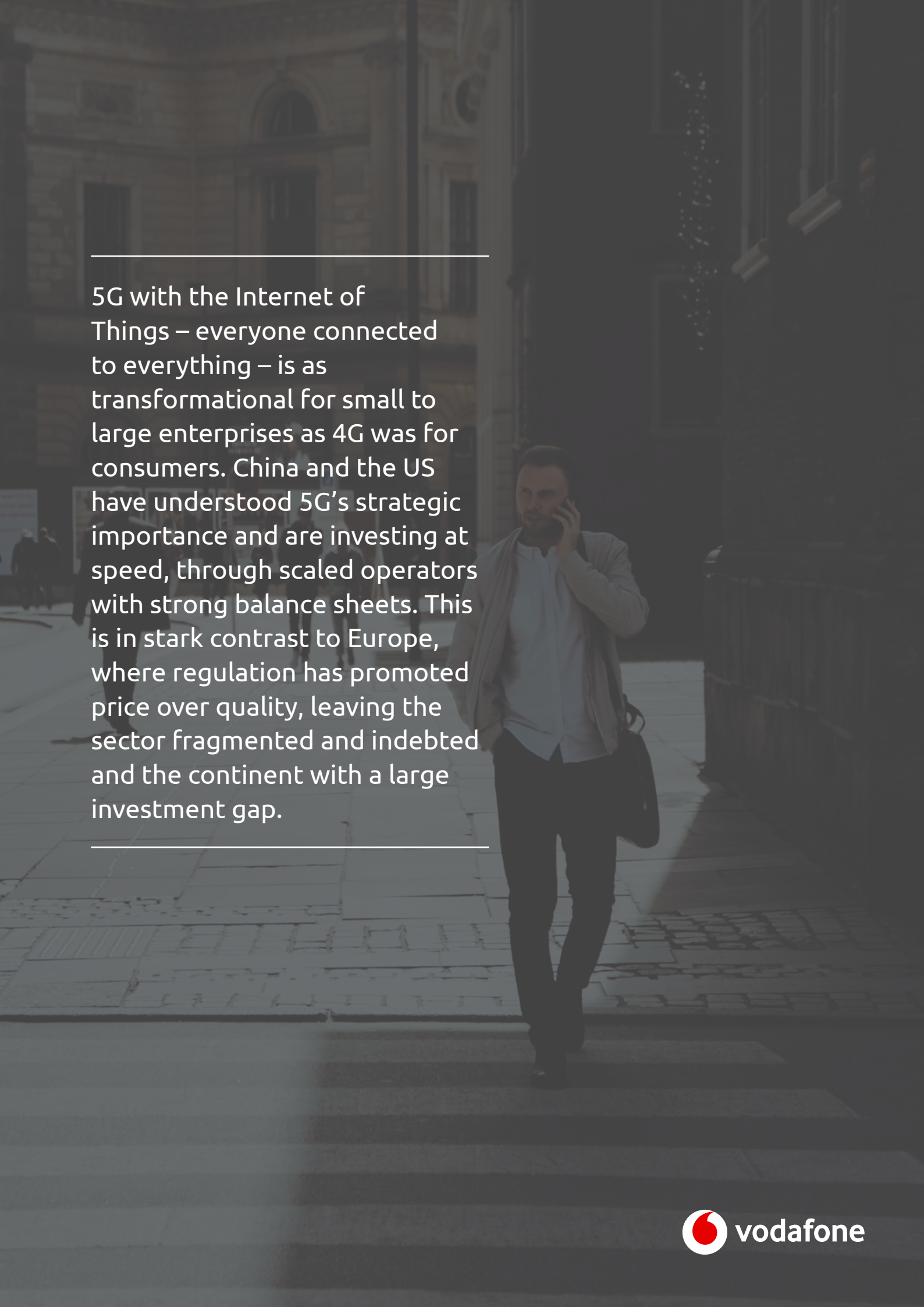
Securing the 5G Eco-system In Europe

vodafone



5G with the Internet of Things – everyone connected to everything – is as transformational for small to large enterprises as 4G was for consumers. China and the US have understood 5G's strategic importance and are investing at speed, through scaled operators with strong balance sheets. This is in stark contrast to Europe, where regulation has promoted price over quality, leaving the sector fragmented and indebted and the continent with a large investment gap.

vodafone

It is in the interest of European countries to address this situation by:

Promoting quick, cost-effective, and efficient deployment of 5G networks and applications (e.g. smart cities, Industry 4.0), in order to promote future economic growth and the competitiveness of the whole economy, while

Ensuring the security and resilience of Critical National Infrastructure, defending against cyber threats, and protecting the public.

Yet, as regards the ongoing 5G security discussion, and specifically the questions around High Risk Vendors (HRVs), many European countries are faced with the challenge of balancing increasing US pressure to restrict or outright ban HRVs with commitments to accelerate the roll-out of 5G networks. A difficult – if not impossible – trade-off in the near term.

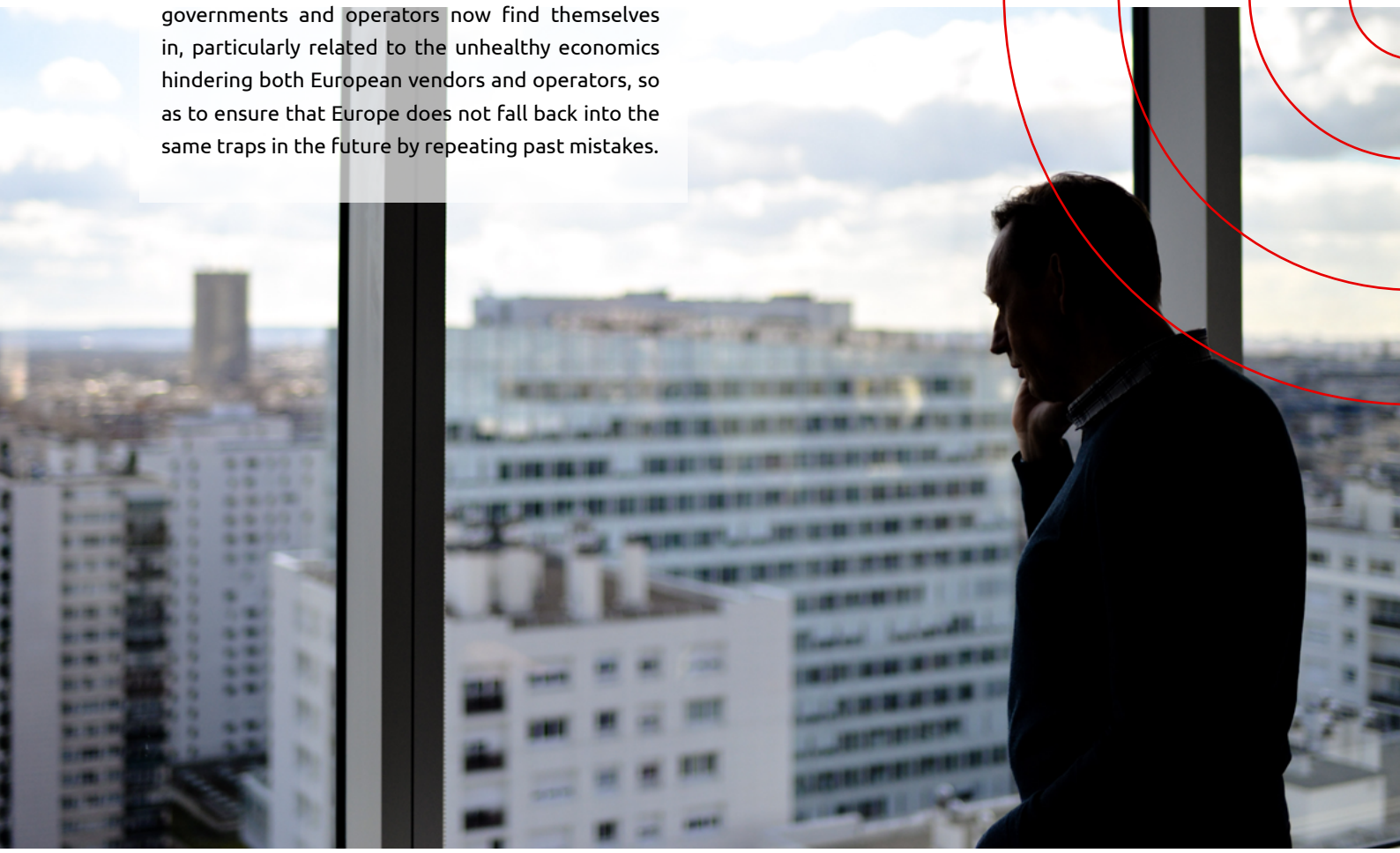
Since 5G in Europe is deployed as an add-on to existing 4G networks, and since presumed HRVs are already significant suppliers to the 4G networks of European operators, any decision to completely ban HRV equipment in 5G – as demanded by the United States – will require the replacement of a significant proportion of equipment in already-installed (2G, 3G, and 4G) networks in Europe. Europe's starting point is, in that sense, fundamentally different from that of the US. But even with a much smaller exposure to HRVs in America, the US government is still struggling with its swap-out plans in rural networks. Notwithstanding US pressure on European partners, US domestic action to fully replace HRVs has still not been taken, and discussions are ongoing for a large subsidy program to cover such costs.

In Europe, by contrast, any rapid and comprehensive swap-out undertaking would be practically impossible. It would likely jeopardise and degrade existing mobile connectivity and services for European citizens, reduce the resilience of Critical National Infrastructure, and imply billions of Euros in additional costs for taxpayers. As operators would struggle to manage the fallout, any such decision would force operators to postpone meaningful 5G deployment in Europe for two to five years, reduce their investments in rural deployment (in low profit areas), and/or pass the additional costs onto consumers – or otherwise cut costs for equipment from European vendors already facing significant financial pressure.

Therefore, such drastic "cliff-edge" scenarios come with unacceptable risks to European citizens and the continent's digitisation ambitions and prospects. They would fail to address existing vulnerabilities while actually worsening resilience. They would also put Europe in an even worse competitive situation on 5G, IoT, and AI compared to China and the US. China is expecting to have ten times more extensive 5G deployment than the EU by end of this calendar year, whereas the US 5G network will be three times that of the EU. China, and to a lesser extent the US, already have a head-start in 5G applications compared to Europe, which does not bode well for future European competitiveness. The EU can ill afford to lag even further behind.

To overcome this, any viable solution will require strategic repositioning and rebalancing of the dependence on a limited pool of suppliers through gradual, medium, and long-term actions. By necessity, this implies also addressing the root causes of the unwarranted situation that European governments and operators now find themselves in, particularly related to the unhealthy economics hindering both European vendors and operators, so as to ensure that Europe does not fall back into the same traps in the future by repeating past mistakes.

The roadmap of actions outlined here would align with the key elements of the EU 5G Security Toolbox and with the approach already pursued by some key European partners. Importantly, it would allow European governments to achieve both accelerated 5G deployment and diligent implementation of the European Union's new 5G security toolbox.



"China, and to a lesser extent the US, already have a head-start in 5G applications compared to Europe"

I.

RISK-BASED APPROACH

Protect the most sensitive part of the network (Core):

1.

Only use trusted suppliers with a proven track record in the core, which is the most sensitive part of the network.

Network architecture, as per international standards, differentiates between the radio access networks, so-called RAN (i.e. the antenna equipment in the base stations) and core networks (data centres, where customer directory and other sensitive information resides). None of this will change with 5G or with the arrival of MEC (Multi-Edge Computing, which would sit in the core). The core of the network aggregates data and performs the most sensitive management functions. From a risk-based security point of view, as advocated by the Department of Homeland Security and as outlined in the EU 5G Risk Assessment, the core network is the most pressing area to address.

Resilient Network Operations & managed services

Network operations (and the OSS provided by the vendor for the respective network element, e.g. RAN OSS, Core OSS, and Transport OSS etc.) provide full visibility of the functioning of the network and are therefore considered of high sensitivity from a security and cyber-defence point of view. . In the EU 5G Risk Assessment, network operations are deemed to be at the same risk level as core networks. Operational Support Systems (OSS) and associated Element Managers provide access to network nodes for configuration and performance management, maintenance and troubleshooting as well as software release upgrades. OSS are high critical network systems due to remote access connectivity and interfaces to large number of sites, therefore the operation of the OSS should always be in-sourced and managed by the operator.

Most serious operators at scale in Europe already insource their network operations (1st and 2nd line support) and sensitive aspects of network management such as network software deployment, OSS upgrades, tools and database upgrades. At the same time, some vendors (including Ericsson) offer a range of managed services to support operators in areas such as site built, site installation, field maintenance and fault management. Managed services should only be allowed under the condition that such services are provided from vendor facilities at home, in Europe which are fully complaint to strict security policies under contractual terms.

"In the EU 5G Risk Assessment, network operations are deemed to be at the same risk level as core networks"

2.

3. Identify limited geographically sensitive radio areas

Based on the identification of specific targeted geographical zones (e.g. military establishments, government institutions, Parliament, national agencies, and so forth), operators are required to limit their use of HRV radio equipment to service these areas.

To be clear, this is questionable from the point of view of security (there is encryption of all traffic and customer data between device/phone and core, with gateways/firewalls between core and radio). However, such measures – provided they are very limited in scope and coverage – may be deemed by some governments as additional precautions to protect metadata information around movements of high profile individuals or inside military bases, and to create comfort for security allies.

In summary, the three key risk-based decisions mentioned above can be taken without significant delay. However, the decisions will have to provide for an adequately long transitional period from the enactment of the decisions to their entry into force, so as to ensure that the measures do not negatively impact European citizens. Also, given the one- off costs (swap in core networks) and additional expenditures of running networks (sensitive zoning), some funding will be warranted through the use of Universal Service Funds or proceeds from auctions. However, the cost of swapping out core equipment (related to 2G, 3G, 4G, and 5G) is relatively limited compared to the overall equipment costs. With 5G stand alone deployment coming, modernisation of the core is already in the roadmap of most operators over the next few years. Therefore, provided adequate time is allowed to implement such a decision, it should be feasible to execute.

II.

RAISING THE BAR ON SECURITY IN THE LONGER TERM

"In the future, only equipment and software that have been evaluated and certified to meet EU standards should be deployed in European networks"

4. Establish a European wide security assurance regime – alongside international cooperation and robustness on common standards & certification – for all network equipment and related software.

In the future, only equipment and software that have been evaluated and certified to meet EU standards should be deployed in European networks. This requirement should apply to all vendors.

Of course, exactly how to certify compliance against common standards should follow a risk-based approach with regard to the function or component that becomes the target of evaluation. Less sensitive functions/components could be subject to more lenient treatment, through audits of software engineering processes (to reduce risk of software glitches), whereas all sensitive (or critical) functions/components would be subject to detailed evaluations (including source code).

To ensure that such audits and detailed evaluations are robust, and applied with equal rigour throughout Europe, it is preferable that one or at most a handful of test centres are set up to service all of Europe, while ensuring close alignment with each EU Member State's national authorities and intelligence services.

Such a new regime could be established within a timeframe of two to three years, depending on the speed by which the EU can make progress on its proposed toolbox.

Take a more holistic stance to security

.5

With 5G becoming a ubiquitous system whereby everyone and everything gets connected, focusing solely on the security of public networks (or even more narrowly on the security of network equipment) would be insufficient, if not directly misleading at times. There is a risk that security, including related cost, is not factored effectively into countries' industrial strategies and related policy decisions (competition, spectrum, network sharing, IoT policy framework etc.).

Security becomes more and more horizontal the more that sectors, industries (large and small) and communities get connected. Those who are new in the digital sphere have less experience regarding security and may not take the same precautions. A holistic approach allows us to reduce and contain damaging effects insofar as possible. A holistic approach also helps to streamline security and find the appropriate balance of voluntary vs. mandatory requirements. All stakeholders have a responsibility and need to play their part.

Governments and the private sector will also need to invest more heavily in cyber-defence, as well as to work in an increasingly collaborative way to fight off cyber-attacks, with the state providing insights and support for both the prevention and remediation of attacks against all providers of critical infrastructure, including purely private companies. There is also a need for minimum standards of security for IoT devices, as well as private networks, to avoid a proliferation of potentially weak attack vectors.

III.

SYSTEMIC ACTIONS FOR MORE SIGNIFICANT AND SUSTAINABLE CHANGE

All of the actions listed above may prove unsustainable and fail to achieve significant change in the long run, unless there is an enabling environment genuinely conducive for a step-change in security. In order to achieve that, a number of flanking measures are absolutely necessary, some of which will require important changes in current approaches.

"Governments should encourage operators to use multivendor strategies, to the extent this is not already the case"

6.

Governments should support development of a more diverse supply chain

Governments should encourage operators to use multivendor strategies, to the extent this is not already the case. While justified from a resilience point of view, this will require either:

- ***Operators agreeing to use different vendors (note: requires coordination by government authorities and may pose problems from a competition point of view) or***
- ***Operators having at least two different vendors in each operator's network (note: this is unlikely to be economically viable in smaller EU Member States or countries with low ARPU/low RoI).***

The basic challenge to diversify the supplier base, however, remains the lack of vendor options. In practice, over the last decade, the vendor space has collapsed, leading to only four credible radio equipment vendors in Europe, two of which are Chinese vendors. For core systems, the situation is marginally better due to availability of additional US vendor(s).

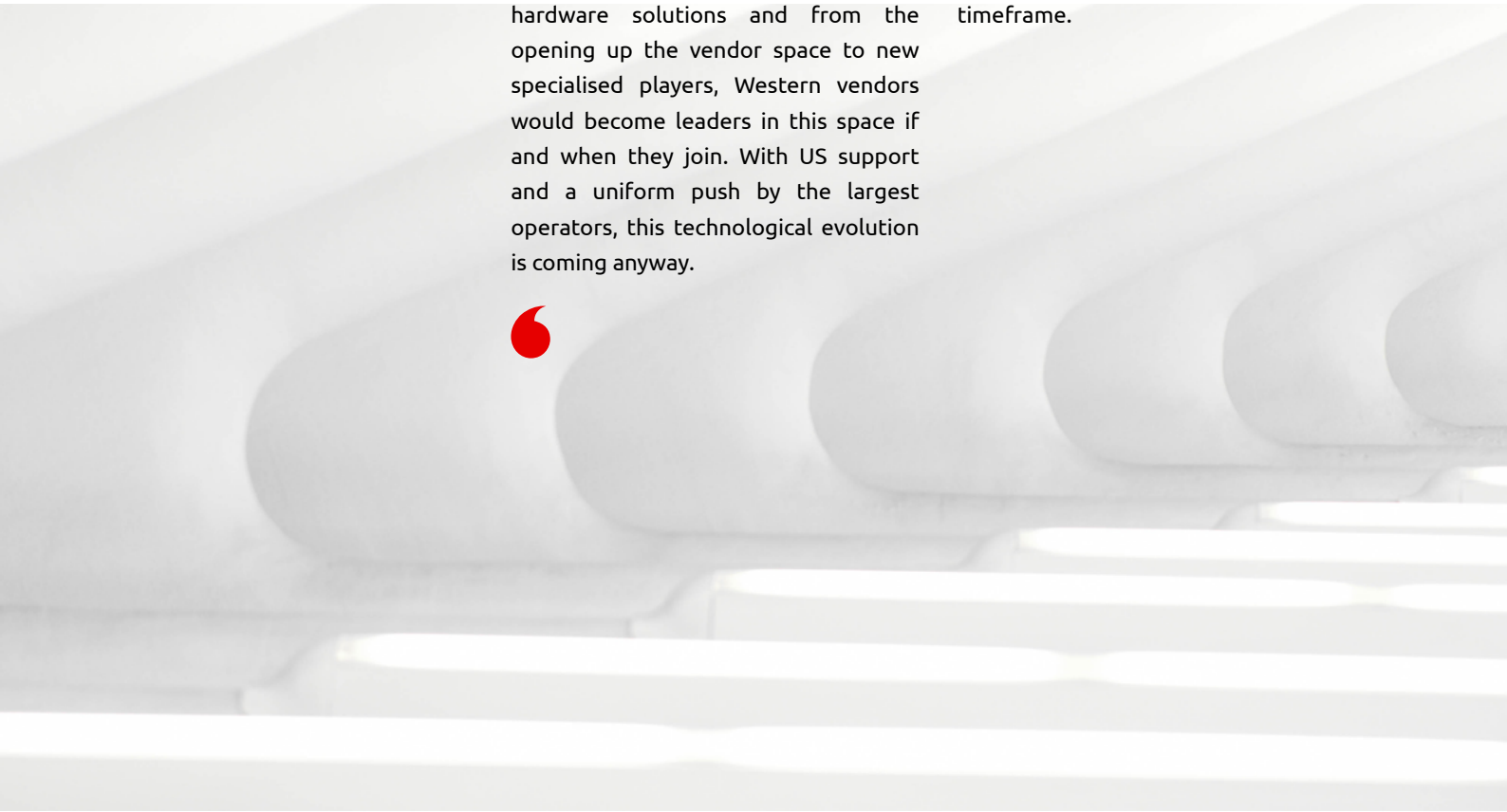
7. Opening up for new players and new optionality through OpenRAN

To address the lack of supplier diversity for network equipment, which lies at the heart of the concerns over resilience of critical national infrastructure, there is an acute need to promote a new ecosystem of niche suppliers to supplement the large vendors, especially for radio equipment and software.

OpenRAN is the most promising route to achieve this over the next few years, and is already in pilot stage in the UK, Ireland and the US, as well as in a few other countries. While existing vendors stand to lose in the short term from moving away from bundled software-hardware solutions and from the opening up the vendor space to new specialised players, Western vendors would become leaders in this space if and when they join. With US support and a uniform push by the largest operators, this technological evolution is coming anyway.

US and European governments should therefore encourage future industrial strategy to include subsidies for R&D and the piloting and deployment of OpenRAN. They should also support start-ups in radio software, much like the US Congress has in proposing to allocate more than USD $500 million in support for OpenRAN.

Governments should also encourage OpenRAN deployment in rural and grey spot areas of their countries, thereby achieving increased 4G coverage by utilising available funds to subsidise deployment by operators. This could also be launched in a reasonably short timeframe.



8

Market pressures and economics of telecommunications

The poor economics of European vendors are intrinsically linked to the equally poor economics of European operators.

In fact, as a sector, European telecom's ROIC already falls short of WACC. It is the worst performing sector on European stock markets over the last 5 years. Since the financial crisis in 2007/08, unlike their US or Chinese peers, European telco revenues have not recovered; instead, prices have fallen more than any other sector in Europe. As a result, Europe struggles with an investment gap, despite EU operators having capital intensity on par with, if not even higher than, the US and China.

This situation is the principal reason why 5G is being rolled out more slowly in Europe than in China or the US. It is also one of the reasons why vendors continue to struggle, especially those dependent on Europe for a significant proportion of their sales.

Therefore, to ensure a healthier vendor space and to drive higher investments in security in the long term, greater emphasis on security must be backed up with economic policies and regulations that put a premium on telco quality and prioritises investments in security. Currently, these policies are driven by short-term objectives of price deflation or otherwise raising funds for treasuries through spectrum auctions.

At the very least, European governments should - in return for investments in security and gradually more robust security requirements - be open to reducing license and spectrum fees. Additionally, governments should reduce auction expenditures for operators (as in China) and automatically extend licences through perpetual licenses (provided license conditions are complied with, as in the US), and alleviate other telco-specific fiscal burdens on those operators complying with high levels of security requirements. In addition, governments could significantly ease infrastructure deployment and reduce the costs thereof. A key action will be to promote network sharing between operators.

The European Commission and national governments also need to refrain from artificially injecting new entrants – through subsidies from either discriminatory spectrum set-asides or as part of competition remedies – that are financially unsustainable or will otherwise lead to market destruction. Sub-scale operators, without the ability to drive investment competition, should not be prevented from exiting and cannot continue to get regulatory holidays with regards to telco requirements or security.

More fundamentally, as long as the telco economic pie is shrinking through government-driven price deflation and the same or greater number of operators are all taking a piece, progress will be difficult. All operators are induced to enter into a vicious circle of chronic underinvesting in quality and security, while squeezing any margin out of the vendors. This, in turn, will undermine the profitability of European suppliers and be counterproductive to the vendor diversity and resilience the sector needs.