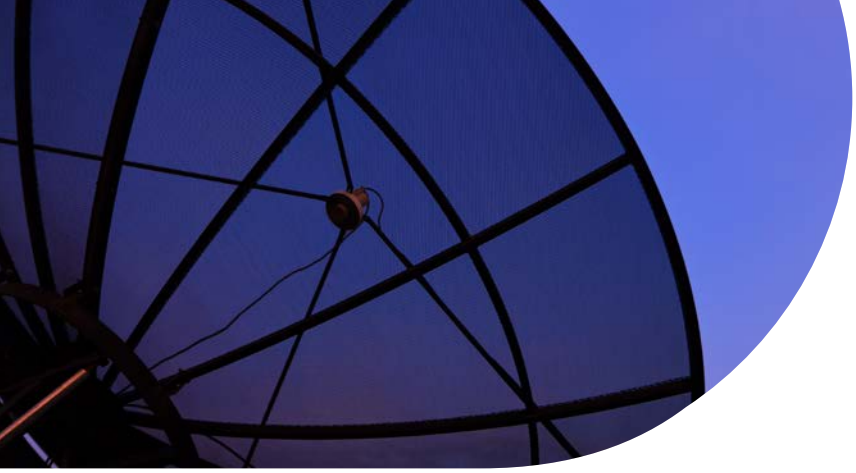

ALLEN & OVERY

High risk vendors in the telecommunications sector: recent developments in the EU, UK, the Netherlands and Belgium

During 2020, across many of the EU Member States and in the UK, restrictions related to so-called "high risk vendors" (**HRVs**) in the telecommunications sector were announced. In the UK, in November 2020, the UK Government introduced the Telecommunications (Security) Bill[1] (the **Bill**) into the UK's Parliament. The Bill seeks to introduce a new regulatory framework for telecommunications security in the UK. The Bill would place stronger security-related duties and responsibilities on telecoms companies and would grant Ofcom, the UK's communications regulator, new enforcement powers. Additionally, and building on the UK Government's previous announcements in relation to so-called HRVs, the Bill would give the Secretary of State powers to impose directions on "public communications providers" (**Providers**)[2] in relation to HRVs, which the Bill refers to as "designated vendors". The Bill was accompanied by a roadmap[3] relating to the removal of HRVs from the UK's telecoms network (the **Roadmap**) and a 5G supply chain diversification strategy[4] (the **Strategy**). Similar measures to the Bill have been adopted or will be adopted in the Netherlands and Belgium.

In this article, we examine the key features of the Bill relating to "designated vendors", the Roadmap and the Strategy. We also outline the Dutch and Belgian governments' recent legislative responses to the issues created by HRVs, and set out the EU-level backdrop.

The background to the Bill

The Bill comes after a period of considerable uncertainty surrounding the UK's policy towards HRVs and telecoms security issues more generally. The UK's Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden, has stated that the Bill is intended to "*give the UK one of the toughest telecoms security regimes in the world*".[5] Importantly, the Bill comes at a time when the UK is conducting a major upgrade of its digital infrastructure[6] against a backdrop of an increase in cyber-security threats[7] and after a long and sometimes fraught debate around the extent of Chinese technology company Huawei's presence in the UK's telecommunications infrastructure.

1. The Telecommunications (Security) Bill 2019-21 (available here: https://services.parliament.uk/bills/2019-21/telecommunicationssecuritybill.html)
2. This includes companies such as BT, Vodafone and Virgin Media that provide networks and/or services that are wholly or mainly used by the public.
3. UK Government, Press release, Roadmap to remove high risk vendors from telecoms network, published 30 November 2020 (available here: https://www.gov.uk/government/news/roadmap-to-remove-high-risk-vendors-from-telecoms-network)
4. UK Government, Guidance, 5G Supply Chain Diversification Strategy, last updated 7 December 2020 (available here: https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy)
5. UK Government, Press release, New telecoms security law to protect UK from cyber threats, published 24 November 2020 (available here: https://www.gov.uk/government/news/new-telecoms-security-law-to-protect-uk-from-cyber-threats).
6. UK Government, Press release, Forging a 5G and full fibre broadband future for all, published 23 July 2018 (available here: https://www.gov.uk/government/news/forging-a-full-fibre-broadband-and-5g-future-for-all).
7. See, for example, GCHQ's characterisation of the cyber threat (available here: https://www.gchq.gov.uk/information/cyber-threat), the UK's National Cyber Security Strategy (available here: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021) and various UK National Cyber Security Centre reports in relation to cyber threats from Russia and China. (available here: https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices and here: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign)

The Bill's two-stage process: "designation notices" and "designated vendor directions"

In relation to "designated vendors", the Bill would create new national security-related powers through the insertion of new provisions into the Communications Act 2003, which sets out the current regulatory framework for the telecommunications sector in the UK. A two-stage process is envisaged by the Bill. First, the Secretary of State would designate a person as a "designated vendor" by issuing a "designation notice" (a **Notice**). This would then give the Secretary of State the power to give directions to Providers through a "designated vendor direction" (a **Direction**) regarding how Providers can use the "designated vendor". Importantly, neither a Notice nor a Direction requires Parliamentary approval. Both must be laid before Parliament, though not if the Secretary of Security considers that such a step would be contrary to the interests of national security.

The Bill provides that a Notice can only be issued if the Secretary of State considers that the Notice is "necessary in the interests of national security". The Secretary of State, in making a decision, may have regard to a range of factors relating to the person being considered for designation, including:

– the nature of the goods, services or facilities that are or might be supplied, provided or made available by the person;

– the quality, reliability and security of those goods, services or facilities or any component of them (including the quality, reliability and security of their development or production or of the manner in which they are supplied, provided or made available);

– the reliability of the supply of those goods, services or facilities;

– the quality and reliability of the provision of maintenance or support for those goods, services or facilities;

– the extent to which and the manner in which goods, services or facilities supplied, provided or made available by the person are or might be used in the UK; and

– the extent to which and the manner in which goods, services or facilities supplied, provided or made available by the person are or might be used in other countries or territories.

Importantly, the identity of the person under consideration for designation, including the country or territory of their registered office, the identity of the persons who own or control them and the degree to which any of those persons might be susceptible to being influenced or required to act contrary to the interests of the UK's national security, will be taken into consideration. Supply chains will also be considered as the factors include the identity of the persons concerned in the development, production and supply of goods, services and facilities, as well as persons providing associated maintenance or support. As "national security" is undefined and the list of factors is wide-ranging and non-exhaustive, the Secretary of State will have considerable latitude when deciding to issue Notices.

Prior to a Notice being issued, the Secretary of State is required to consult the person or persons named on the Notice, as far as it is reasonably practicable to do so, unless that consultation would be contrary to the interests of national security. Notices can be varied or revoked.

Once a Notice has been issued, the Secretary of State may give a Direction to a Provider. Such a Direction can only be given if the Secretary of State considers that the Direction is necessary in the interests of national security and the requirements imposed by the Direction are proportionate to what is sought to be achieved by it. The Direction may impose requirements on the use of goods, services or facilities that are supplied, provided or made available by the "designated vendor". For example, the requirements could impose a prohibition or restriction on the use of goods, services or facilities provided or made available by the "designated vendor", requirements to modify such services, or requirements in respect of the way in which such goods, services or facilities may be used. In short, the power envisaged in the Bill relating to the content of a Direction is wide-ranging and confers considerable discretion on the Secretary of State.

Before a Direction is given, the Secretary of State must consult the Provider(s) that would be subject to the proposed Direction and the relevant "designated vendor", as far as it is reasonably practicable to do so, unless that consultation would be contrary to the interests of national security. A Provider is required to comply with a Direction, and Directions can be varied or revoked.

An illustrative Notice and Direction have been published in relation to Huawei[8] which reflect the matters on which the Secretary of State "*is presently minded to consult Huawei and public communication providers upon the enactment of the Bill*".[9]

The Bill also gives the Secretary of State the power to require a Provider to produce a plan setting out the steps it intends to take to ensure compliance with a Direction and the timing of those steps (a **Compliance Plan**). The Secretary of State will have the power to specify the period within which a plan must be provided to Ofcom and the Secretary of State.

8. Draft Designation Notice under section 105Z8 of the Communications Act 2003, designating Huawei for the purposes of a designated vendor direction (available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/939035/Huawei_Draft_Designation_Notice-c.pdf)
9. UK Government, Policy paper, Telecommunications (Security) Bill: Illustrative designated vendor direction and designation notice, published 30 November 2020 (available here: https://www.gov.uk/government/publications/telecommunications-security-bill-illustrative-designated-vendor-direction-and-designation-notice)

Monitoring, enforcement and non-disclosure requirements under the Bill

The Bill gives powers to the Secretary of State and Ofcom to monitor implementation of Directions, backed up by a maximum penalty of GBP10 million, or GBP50,000 per day in cases of continued contravention, in the case of non-compliance with the monitoring regime by Providers.

The Bill also provides the Secretary of State with the power to require information from relevant persons to support the Secretary of State's monitoring efforts and decision making. A notice is required in relation to such requests and contravention of that notice carries a maximum penalty of GBP10m, or GBP50,000 per day in cases of continued contravention.

The Bill contains robust enforcement provisions that allow the Secretary of State to determine that a Provider is contravening, or has contravened, a requirement in a Direction or a requirement in relation to a Compliance Plan. In such circumstances, the Secretary of State can issue a notice of contravention which specifies the remedial steps required of the Provider and the penalty that the Secretary of State is minded to impose. That penalty must be appropriate and proportionate to the contravention in respect of which it is imposed. Where a Direction is said to have been contravened, the maximum value of the penalty is 10% of the Provider's relevant turnover during a specified period, or GBP100,000 per day in respect of a continuing contravention. In the case of a contravention of a Compliance Plan, it is GBP10m, or GBP50,000 per day. It is clear that the penalties for breaching a Direction are intended to have a deterrent effect, and the UK Government has stated that it will take a "robust" approach to monitoring compliance.[10]

Before a notice of contravention is finalised through the issuance of a "confirmation decision", the Secretary of State must allow the Provider to make representations. Once the period for those representations has passed, the Secretary of State may decide not to take any further action or to issue a "confirmation decision". A "confirmation decision" must be provided without delay, include reasons and may require immediate remedial actions to be taken and/or the payment of a penalty. A Provider would be placed under a duty to comply with the "confirmation decision" which is enforceable in civil proceedings.

Furthermore, the Bill provides the Secretary of State with powers to give an "urgent enforcement direction". Such a direction could be given in circumstances where, for example, the Secretary of State determines that there are reasonable grounds for believing that a Provider is contravening, or has contravened, a requirement imposed by a "designated vendor direction", or the contravention has resulted in, or creates a risk of, a serious threat to national security and it is appropriate for the Secretary of State to take action. The "urgent enforcement direction" will specify the steps that the recipient is required to take to comply with the requirement or to remedy the consequences of the contravention. A recipient of an "urgent enforcement direction" would have a duty to comply, which is enforceable in civil proceedings.

Finally, in relation to "designated vendors", the Bill provides the Secretary of State with powers to require the non-disclosure of the existence or content of certain documents and consultations where their disclosure is determined to be contrary to national security. The penalties for non-compliance with the non-disclosure obligations are a maximum penalty of GBP10m, or GBP50,000 per day in cases of continued contravention.

10. Ibid

The UK's Roadmap and the Strategy

The Roadmap and the Strategy were published shortly after the Bill. Together they set out the UK Government's approach to expediting the removal of Huawei's equipment from the UK's 5G network and ensuring that the UK does not become, in Huawei's absence, overly reliant on any other suppliers. Two important elements announced in the Roadmap and the Strategy are that the installation of any of Huawei's equipment in the UK's 5G network will be prohibited from the end of September 2021, and GBP250m has been pledged to create a "more diverse, competitive, and innovative supply market for telecoms".[11] This money will be spent on a number of projects including funding a new Open RAN trial with NEC (a Japanese telecoms vendor) and establishing a National Telecoms Lab. Additionally, the UK Government will prioritise influencing standard-setting bodies and taking a leadership role internationally to establish a competitive and sustainable supply chain.

The EU Toolbox as the guidebook

Before we turn to the Dutch and Belgian regimes, it is worthwhile to set out the policy backdrop at the EU-level. On 29 January 2020, following a consultation process involving all EU Member States, the European Commission endorsed the "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures" (the **EU Toolbox**).[12]

The EU Toolbox aims to bolster a coordinated European approach in the area of 5G security, and identifies a common set of measures to address the main cybersecurity risks. This includes the introduction of additional security measures to mitigate the risk of interference by a non-EU country in the 5G supply chain, for which the EU Toolbox advances four criteria: (i) the presence of a strong link between the supplier and a government of a given non-EU country; (ii) the non-EU country's legislation, especially "*where there are no legislative or democratic checks and balances in place*" or in the absence of data protection agreements with the EU; (iii) the corporate ownership of the supplier; and (iv) the ability of the non-EU country to exercise any form of pressure on the supplier. The EU Toolbox does not, as such, target any particular countries.

It is now for the individual Member States to adopt the necessary legislation to implement the recommendations set out in the EU Toolbox. The European Commission has recently urged that this process be completed by Q2 2021.

11. UK Government, Press release, Roadmap to remove high risk vendors from telecoms network, published 30 November 2020 (available here: https://www.gov.uk/government/news/roadmap-to-remove-high-risk-vendors-from-telecoms-network)
12. European Commission, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures (available here: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures)

The Dutch Telecommunications Security and Integrity Decree

Against the backdrop of this EU Toolbox, and almost simultaneously with the introduction of the Bill, the Dutch government published its "Telecommunications Security and Integrity Decree" (the **Decree**).[13] The Decree contains a legislative basis for regulating mobile network operators (MNOs) in order to address national security risks. The key aspects of the Decree will be implemented through individual decisions by the Minister of Economic and Climate Affairs (the **Minister**).

The Decree provides that the Minister can impose an obligation on MNOs to "*only use trusted suppliers in the most sensitive parts of the network designated by the Minister.*"[14] The Dutch Government has noted that this obligation is justified since "*[a]buse of products and services of suppliers in the telecoms sector offers state actors possibilities to spy on […] sensitive information and compromise the national safety of the Netherlands as a result*".[15] The Dutch Government has further stated that this is all the more so since multiple (foreign) countries have legislation in force that can coerce suppliers to cooperate with their national intelligence service. The Dutch Government considers it particularly important to enact rules given the roll-out of 5G in the Netherlands and the perceived vulnerability associated with this technological development.[17]

The envisaged ban on distrusted suppliers does not follow directly from the Decree, instead it must be specified in a decision made by the Minister. In the decision, the Minister can impose a ban if an MNO purchases products or services from a party that:

"a) is a state, entity or person of which it is known or for which there are grounds to suspect that it intends to misuse or take down an electronic communication network or service offered in the Netherlands; or

b) has close links with or is under the influence of a state, entity or person referred to in paragraph (a), or is an entity or person with respect to whom there are grounds to suspect such links or influence".[18]

The Decree has been issued using a provision in the Dutch Telecommunications Act 2012 which contains a general obligation for telecommunication providers to take appropriate technical and organisational measures to manage security and integrity risks for telecommunication networks and services.[19] As such, it is clear that the Dutch Government considers that the imposition of a ban on distrusted suppliers is an appropriate organisational security measure for MNOs.[20] In addition, the Decree provides a basis for further measures by ministerial regulation to increase the resilience of the networks of MNOs.[21] The Dutch Government notes that the power to ban distrusted suppliers has been included as the existing general measures and the envisaged additional measures provide, in the Government's view, insufficient protection for critical parts of the networks of MNOs.[22]

In the explanatory note accompanying the Decree, the Dutch Government states that the Decree provides a basis for controlling the use of network parts of MNOs.[23] As a result, the Government considers that an individual decision to designate a distrusted supplier and sensitive network parts results in an interference with the right to the peaceful enjoyment of one's possessions within the meaning of Article 1 of the First Protocol of the European Convention of Human Rights (**ECHR**), which is a qualified right.[24] Consequently, the Dutch Government has stated that it may be necessary to compensate MNOs for certain losses to the extent that doing so is necessary to achieve a fair balance within the meaning of the ECHR.[25] In this regard, the Dutch Government recognises that the Dutch law principle of equality of public burdens may also lead to an obligation to compensate certain losses incurred by MNOs.[26]

13. Originally named the "Besluit veiligheid en integriteit telecommunicatie"
14. Article 2, section 2 Decree (available here: https://wetten.overheid.nl/BWBR0042843/2020-03-01)
15. Explanatory note Decree, page 3 (available here: https://zoek.officielebekendmakingen.nl/stb-2019-457.html)
16. Ibid
17. Explanatory note Decree, pages 3-4
18. Article 2, section 2 Decree
19. Article 11a.1, section 4 Telecommunications Act
20. Explanatory note Decree, page 3
21. Article 2, section 1 Decree
22. Explanatory note Decree, pages 3-4
23. Explanatory note, page 5
24. Explanatory note, page 6
25. Explanatory note, page 8
26. Ibid

The proposed Belgian *ex ante* authorisation regime

On 22 June 2020, to implement the EU Toolbox, the Belgian National Security Council decided on the principles for additional security measures to restrict HRV equipment in Belgian 5G networks.

Following that decision, on 2 December 2020, the Belgian telecom regulator published pre-draft implementing legislation (the **Belgian Draft Legislation**) and arranged a public consultation on the proposed texts. The Belgian Draft Legislation seeks to amend the Belgian telecom laws to provide for a system of ex ante authorisation, whereby telecom operators must request and obtain an authorisation from the authorities prior to starting to use 5G network infrastructure. In line with the decision of the National Security Council, it provides for a complete ban on HRV equipment in the most sensitive parts of the network and in (yet to be defined) "sensitive zones", as well as a 35% size-cap in less sensitive parts of the network.

The Belgian Draft Legislation does not provide clarity on the classification of HRVs. Instead, it envisages that the classification of a particular supplier as an HRV (and thus the trigger for restrictions to apply) will depend on an individual decision taken by the authorities in response to an individual authorisation request for a specific 5G network. The decision will be made on the basis of both technical (following advice of the Belgian telecom regulator) and national security (following the advice of the national security services) considerations. In addition, the identification of sensitive areas (where a complete ban on HRV equipment will apply) remains unclear, and substantive and procedural safeguards for individual authorisation decisions (including possibilities for judicial review) are largely absent from the Belgian Draft Legislation.

In addition, the Belgian Draft Legislation is not entirely clear on the question of whether 4G or older legacy equipment will be subject to the new restrictions. Although it states that mobile networks from the fourth and earlier generations are excluded, the Belgian Draft Legislation does seem to apply to legacy equipment as soon as it is used in a 5G network, seemingly overlooking the fact that 5G networks will need to be integrated with, and build upon, network infrastructure from earlier generations.

As a result, the Belgian Draft Legislation does not appear to live up to its stated purpose of providing clarity and legal certainty to the various 5G stakeholders. Nonetheless, it is interesting to note, firstly, that the Belgian telecom minister has stressed that, in line with the EU Toolbox, the purpose is not to target any particular companies or countries, and secondly, that in addition to the criteria set out in the EU Toolbox, the Belgian Draft Legislation seeks to include one additional criterion for the classification of a particular supplier as an HRV: that is whether the supplier's country of origin conducts an "offensive cyber policy". In that regard, it is interesting to note that published "league tables" of offensive cyber capability are not necessarily led by the countries one might expect.[27]

The public consultation on the Belgian Draft Legislation ended on 31 December 2020. The Belgian telecom minister announced that her cabinet is now processing the feedback provided, will consult with the relevant stakeholders over the next few weeks, and will aim to get the legislation through the Belgian Parliament and published before June 2021.

We will have to wait and see whether Belgium can meet this very ambitious deadline in what has already proven to be a challenging area in which to legislate.

27. See the Economist "A new global ranking of cyber-power throws up some surprises" published on 19 September 2020 (available here: https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises)

4. Conclusion

In the UK, the Bill's powers in relation to "designated vendors" represent a watershed moment in the development of the UK's response to cyber-security threats and national security concerns in relation to the UK's telecommunications network. Notably, the powers envisaged are exceptionally broad, afford considerable discretion to the Secretary of State and are subject to limited Parliamentary oversight. Certainly, we expect the latter point will be a particular focus of debate during the Bill's Parliamentary passage. Industry participants will also no doubt be concerned about the breadth of the requirements that can be imposed, the potentially invasive nature of the UK Government's monitoring powers and the level of due diligence that they may be required to engage in to assess the risks associated with their supply chains.

The Bill has also been introduced at a time when the UK's National Security and Investment Bill is being debated in Parliament. Taken together, these bills create a formidable armoury of new powers for the UK Government to intervene in the operation of the UK's telecommunication sector. All businesses operating in the sector will need to carefully consider the potential impact of the bills on their operations. We expect both Bills to come into force in the first half of 2021.

However, as developments at the EU-level, as well as in Belgium and the Netherlands, illustrate, States are grappling with the issues arising from the use of HRVs in a multiplicity of ways. This makes the compliance and operational task for telecoms companies, especially those operating on a cross-border basis, particularly challenging. It also remains to be seen what, if any, impact the change of presidential administration in the U.S. will have on the approach of European countries in the future to this issue. No doubt this coming year will prove as interesting in this regulatory area as the last.

A version of this article first appeared in WorldECR.

4. Key Contacts

Matt Townsend
Partner, London
Tel +44 20 3088 3174
Mob +44 79 0968 4728
matthew.townsend@allenovery.com

Jonathan Benson
Senior Associate, London
Tel +44 20 3088 1321
jonathan.benson@allenovery.com

Thomas Declerck
Senior Associate, Brussels
Tel +32 2 780 2483
Mob +32 473 573034
thomas.declerck@allenovery.com

UK
CS2102_CDD-62994_ADD-94228