POSITION PAPER

BUSINESSEUROPE

4 June 2019

Cybersecurity of the 5G Ecosystem

KEY MESSAGES

- Welcomes a **coordinated European approach** to uphold cybersecure 5G roll-out that upholds single market principles;
- A **formal structure of information sharing is required** between a multitude of actors (not just those listed within the Cooperation Group of the Cybersecurity Act);
- The **budget of the Digital Europe Programme should be increased** and MFF negotiations finalised as soon as possible;
- The Cybersecurity Act should **prioritise development of schemes supporting the 5G ecosystem;**
- **Security by design** principles should be at the heart of developing 5G infrastructure;
- 5G **source code should not be shared** with 3rd parties outside secure environments;
- The **business community needs to be involved** in the Commission-Member State consultation on 5G risk assessments;
- **Post-development testing could depict a false sense of security** and should not be prioritised as a method to elevate cybersecurity across Europe;
- Ongoing best industry practices should be built upon to create **European Guidelines in relation to cybersecure code development**

BUSINESSEUROPE

POSITION PAPER

CONTEXT

Europe has embarked on a journey to further digitalisation in society. Entire sectors are transforming and through this, new opportunities are being created for businesses to deliver solutions for Europe.

5G is the catalyst of the next phase of this ongoing digital revolution. It will connect billions of machines and enable new technologies, such as: automation, robots, block chain, sensors, Internet of Things (IoT), AI, smart cities, future mobility, industry 4.0, financial services, content services, public services, eHealth. Moreover, 5G will result in more rapid innovations in nanotechnologies/advanced materials and micro-electronics. 5G will also have a major impact on cybersecurity.

At the same time, we must remember that future capacity, functionality, legal environment and industrial policies surrounding 5G networks will ultimately decide at what pace this technology will deliver these expected benefits to Europe compared to other leading regions. We support tech-neutrality in order to bring the benefits digitalisation offers to Europe's citizens and businesses.

Yet as our industries continue to digitalise so have harmful forces. This next phase of the digital revolution could be held back if cyberattacks continue to increase and harm businesses and consumers' trust.

In Europe, cyber-espionage jeopardises up to € 60 billion in economic growth and up to 289,000 jobs.[1] Businesses are increasingly experiencing greater economic and reputational losses through cyber-espionage. As the divide between the digital and the physical spaces increasingly blur, such as through the IoT, the potential threat to citizens and businesses is also growing. In particular, Cyber-espionage is therefore a top concern of reputable businesses around the globe today.

This is even more of a concern when Europe experiences such slow detection rates. It takes Europe three times longer on average to detect a cyber intrusion than the rest of the world.[2] If the digital eco-system that relies on networks of critical infrastructures, software, platforms, devices and even political institutions cannot be better protected through 5G, then Europe will not present itself as a trusted place to do business or invest in.

BusinessEurope welcomes this Commission Recommendation[3] in order to invite Member States to coordinate a European approach to ensure consistent and unfragmented cybersecurity requirements for 5G. These actions should stay within the confines of existing laws and should not set retroactive legislation or go further and fragment frameworks to the detriment of the single market. Particular requirements should not contradict already existing terms and conditions prevailing in existing networks.

[1] ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber-espionage be allowed to hold Europe Back in the global race for industrial competitiveness? Available at: http://ecipe.org/publications/stealing-thunder/?chapter=all

[2] FireEye (2017)

[3] on Cybersecurity of 5G Networks C(2019) 2335 final

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

We urge Member States to place their upmost attention to implementing these recommendations in a coordinated manner. In turn, businesses will play their role in order to increase 5G cybersecurity levels for Europe.

EUROPEAN ACTION

Greater information sharing will only begin at the grass roots level if a safe and structured process exists. **A formal structure is needed** (like RAPEX) that enables cooperation between the Commission, Member States, ENISA, national agencies, businesses and citizens. Not just those outlined within the Cooperation Group as described in the Cybersecurity Act. Businesses currently find it difficult to share information with authorities for them to coordinate reactive measures. We are concerned that sharing information on weaknesses in technology or actual security breaches could be leaked causing economic and reputational damage. The flow of information from state to business also needs to be improved. All risk scenarios and threats relevant to 5G should be covered in any devised structured information sharing process.

The **Digital Europe programme should increase its 9.2 billion EUR budget** as only part of this will be used for cybersecurity purposes – yet more is being asked of Member States through these recommendations. Ongoing **Multi-annual Financial Framework (MFF) negotiations should be concluded as soon as possible** to ensure financial commitments follow political will.

A first step of European cooperation could be demonstrated by **developing cybersecurity schemes in relation to the 5G ecosystem.** However, we do urge caution over making all of these mandatory. This will depend on the objective, application and design of each scheme. Likewise, schemes should only be appropriately developed through a joint effort between industry and the relevant authorities as defined in the Cybersecurity Act. It is industry in the end that will apply these schemes on the ground and thereby contribute to the protection of personal and non-personal data, business IP and critical infrastructure from cyber-attacks and cyber-espionage.

"Security by design" should be utilised as a principle when developing components for 5G infrastructure. This will help the cybersecurity level of the entire 5G ecosystem from the start. Europe's Research and Innovation programmes could provide tools and competence development in this crucial area. This is not limited to just network security (holistically including security of: products, networks, configurations of the network and operations) but indeed all applications linked to the network that deliver sensitive solutions (eg. smart transport, e-health and IoT).

Businesses continue to invest heavily in cybersecurity in order to understand, prevent and limit cyberattacks. This is a key part of our business model as it enables us to sell our products and provide services globally in a safe manner. While the Commission Recommendation is not specific on what businesses should do to elevate 5G cybersecurity many actions resulting from it will have a rebound effect on businesses and make them act. As a mere example, the ongoing debate across Member States surrounding **disclosure of 5G source code rises potential risks**. Depositing source code is not designed to guarantee security particularly in a digital ecosystem that is constantly in flux.

Disclosing the source code which makes 5G operate would require vendors of critical infrastructure and public communication networks to hand over vital IP to 3rd parties for review. The consequences of mandating this transfer and **enabling access to source code outside a secure environment would introduce new security threats** (particularly through uncontrolled leaking), would be a disproportionate measure to increase security and would actually weaken security. Protection of intellectual property is already extensively invested in. Leaving it open to uncontrollable risks would be highly detrimental to this investment.

MEMBER STATE ACTION

The current Recommendation depicts a private consultation between the Commission and Member States to determine a coordinated risk assessment of national 5G infrastructure. Risk assessments carried out at national level may not all be alike. As a result, differing mitigating measures could appear. These measures (eg. third-party certification, tests or conformity checks) will require the full involvement and commitment of entire supply chains, **it is crucial that the business community is part of these Member State risk assessments.** As 5G networks can be included in infrastructure of Operators of Essential Services (OES), as defined by NIS Directive 2016/1148, cooperation between network operators and OES (from the risk assessment to the provision of up-to-date software and hardware that do not contain publicly known vulnerabilities) is strongly recommended. Companies should also have immediate access to the shared toolbox of possible risk management measures to be put in place by 31 December 2019.

While Member States will be key to organising risk assessments of the 5G ecosystem to identify sensitive areas, businesses know that **post-development testing could create a false sense of security.** What is tested in a lab may not match a live network. This stage of testing may be insufficient as it could only reveal a limited representation of an ecosystem at a given moment in a specific configuration. This does not fit to the realities of a hyper connected and dynamic digital economy. If lab-testing does not fully display the actual deployment – which is strongly dependant on adaptations, processes and controls – the results of testing may be inaccurate. Likewise, modern software development builds on continuous deployments of new releases, updates and functionalities. Therefore, tests on one version of the system do not reflect behaviour of that system after it has been altered.

It is also difficult to determine which products, services, processes and vendors should be included in any proposed post-development testing. The 5G ecosystem will include various layers of physical and virtual connections, involving software, hardware and platforms. This will especially be the case as 5G permits critical and massive machine-to-machine communication. Expanding the scope of testing to all of these use cases may further slowdown development of new industrial business cases. If necessary, **BusinessEurope calls on the European Commission to focus on components for 5G infrastructure.**

Overall, we believe that industry can uphold privacy and security by design principles while ensuring cybersecure supply chain management through fully understanding risks and then gauging decisions based on the criteria of those risks. Best practice sharing amongst industry is already taking place. This could be **heightened through**

Commission support for guidelines, developed in direct contact with industry, to encourage similar methodologies to be used across Europe to determine best practices for software development. This would strengthen the robustness and the resilience of both 5G infrastructures and hosted virtual network functions.

* * *