An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

ComReg Response to the National Security Strategy Consultation

Response to Consultation

Reference: ComReg 20/02

Version: FINAL

Date: 13/01/2020

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Additional Information

Approval

Legal Disclaimer

This Response to Consultation is not a binding legal document and also does not contain legal, commercial, financial, technical or other advice. The Commission for Communications Regulation is not bound by it, nor does it necessarily set out the Commission's final or definitive position on particular matters. To the extent that there might be any inconsistency between the contents of this document and the due exercise by it of its functions and powers, and the carrying out by it of its duties and the achievement of relevant objectives under law, such contents are without prejudice to the legal position of the Commission for Communications Regulation. Inappropriate reliance ought not therefore to be placed on the contents of this document.

An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

By email to Contact@nsac.gov.ie

23 December 2019

National Security Analysis Centre,
Department of the Taoiseach,
Merrion Street Upper,
Dublin 2,
D02 R583

RE: COMREG RESPONSE TO THE NATIONAL SECURITY STRATEGY CONSULTATION

To whom it concerns,

On behalf of the Commission for Communications Regulation ("ComReg"), I wish to express support for the development of a National Security Strategy for Ireland, as set out in the public consultation entitled "Public Consultation on a National Security Strategy for Ireland", published by the Department of the Taoiseach on 5 December 2019 ("the Consultation"). In particular, ComReg welcomes that the Consultation will lead to a strategy that will set out a whole of Government approach, as no one Government Department or agency has full responsibility for national security. Following is ComReg's submission to the Consultation which is in line with the suggested structure: National Security concerns, goals, strategy and capacity.

Background

At present, all undertakings providing public communications networks and publicly available communications services in the State are required to take appropriate technical and organisational measures, having regard to the state of the art and in order to ensure a level of security appropriate to such risks and to prevent and minimise the impact of security incidents on users and interconnected networks. In meeting their obligations, providers of such networks and services are also playing a supportive role in making internet-based information services more robust and secure.

ComReg has certain powers to monitor providers' compliance with their requirements and to issue directions to providers for the purpose of ensuring their compliance with their obligations as outlined herein, where objectively justified and proportionate to do so.[1] In 2018, ComReg established a new unit – Network Operations Unit, with limited resources, whose focus is on monitoring and ensuring providers' compliance with their obligations in respect of network resilience and security. To be

[1] Please see regulations 23 and 24 of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011). The Framework Directive, of which S.I. 333/2011 is based, has been superseded by the European Electronic Communications Code, Directive (EU) 2018/1972. Articles 40 and 41 will come into force when the Directive is transposed into Irish law. The Directive is due to be transposed into Irish law by the end of 2020.

effective in its role, the Network Operations Unit has established good working relationships with other State agencies, such as the National Cyber Security Centre, as network resilience and security can involve working and collaborating with other State agencies and government departments.

ComReg views the security and resilience of electronic communications networks as a matter of key importance, especially as those networks continue to grow and as services provided through those networks become ever more widespread and essential to the socio-economic activity of the Irish economy. The ever increasing reliance on connectivity, by Irish consumers and business alike, means that the security of communications networks has become a matter of critical concern of all users, now and in future.

ComReg for its part has a statutory responsibilities for the regulation of all providers of public communications networks and publicly available communications services in the State: from next generation fibre to the home (FTTH) broadband services, National Broadband Ireland, fixed wireless broadband services, to future mobile broadband services such as 5G.

In its role in the management of Ireland's spectrum natural resources, ComReg has begun making spectrum suitable for 5G networks and services. In 2017, ComReg successfully assigned 350 MHz of spectrum in the 3.6 GHz band. Currently, ComReg is developing a multi-band spectrum award process for the assignment of 470 MHz of harmonised spectrum in the 700 MHz, 2.1 GHz, 2.3 GHz and 2.6 GHz bands. This release of spectrum will increase the availability of harmonised wireless broadband (WBB) services in Ireland by 46%[2].

ComReg would expect the award of this spectrum to be particularly suitable for enabling advancements in current 4G services and the delivery of new 5G services. In total, ComReg will assign up to 820 MHz of spectrum suitable for 5G networks and services. This will significantly enable the market to provide improved services to meet increasing consumer demand for mobile data and new services.

The ever changing telecommunications technologies which facilitate the development and growth of today's interconnected society, are transforming the way Irish people engage in their everyday lives. Today's economic and societal development is strongly related to the existence of secure and resilient telecommunication networks, providing the infrastructure needed for society and business to operate. ComReg's recent Quarterly Key Data Report[3] bears this out, with fixed broadband subscriptions increasing to 1.45 million, which is an increase of 2.5% since last year. There is an increase in consumer take-up of higher speed fixed broadband products, 46% of which are for broadband services of 30 – 100 Mps and 34.9% are for broadband services delivering speeds greater than 100 Mps. The average monthly data usage per fixed broadband subscription 195.6 GB for residential subscriptions and 119.9 GB for business subscriptions, this an increase since 2018 of 18% and 46% respectively. ComReg's has found that 59.8% of all mobile subscriptions are actively using 4G networks, up 55.3% from 2018, with the average mobile user using 7.2 GB of data per month, up 18.8% from 2018.

[2] ComReg Document 19/124, Proposed Multi Band Spectrum Award – Response to Consultation, The 700 MHz duplex, 2.1 GHz, 2.3 GHz and 2.6 GHz Bands, 20 December 2019.
[3] ComReg Quarterly Key Data Report Q3 2019, document 19/112, 12 December 2019.

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation

Next generation telecommunications networks, including 5G networks, are set to become the backbone for essential services such as energy, transport, banking, health and other utilities. The European Commission makes much the same observations in its Recommendation on Cybersecurity of 5G networks, published on 26 March 2019[4]. The complexity of future networks present new risks and security challenges for providers of public communications networks and publicly available communications services.

Concerns

As set out in the section above, Background, there is a growing reliance on public communications networks and publicly available communications services, both fixed and mobile. Next generation networks, such as 5G, are set to enable greater socio-economic activity and become the backbone for essential services, utilities, banking and health, to name but a few.

Publicly available communications networks and services play, and will continue to play, a significant role in Ireland's economic development and in its national security. The complexity of and the reliance on the technologies used to deliver networks and services to businesses and the public, increases the vulnerability to the resilience and security of those networks and services. The technology evolution which 5G promises will include:

- the virtualisation of various network elements, potentially resulting in network elements existing and/or being controlled from outside of the State;
- an increase in connectivity to facilitate Machine-to-Machine ("M2M") communications, Internet of Things ("IoT");
- a greater use of Open Source Software ("OSS") within networks; and
- use of third country suppliers of IoT/M2M devices, software and cloud hosting;

The change in network architecture required for 5G outlined above, while yielding benefits to society and the economy, will also increase the attack area of the network. It will also result in an increase in threats to and vulnerabilities within a network.

The European Union Agency for Cybersecurity (ENISA) recently published a Threat Landscape for 5G Networks[5]. In this report, of all the threat agents, ENISA has called out Nation States (or State Actors) as the threat agent group of importance, due "both to its ability to compromise future 5G Network and its potential motivation to do so". The report highlights that vendors of 5G components have the capacity to cause devastating attacks to the operation of self-developed components, especially when governments influence them. Given the expected importance of 5G to society and the economic activities of any country, it is likely that 5G networks will be a target of a State Actor-sponsored attacks.

There is a growing need for State agencies to have access to and an ability to discuss national security intelligence. The State and its agencies all have a role to play in ensuring State security, this will be most effective if there is a mechanism in place to facilitate access to and inter-agency discussion on national security intelligence. Given the importance of telecommunications services (current and

[4] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks C/2019/2335
[5] ENISA threat landscape for 5G Networks, 21 November 2019.

future) to the State and its potential to attract threats to Irish national security, ComReg is ready to play a role in national security matters. In order to fulfil its role, ComReg would welcome a mechanism to facilitate access to and inter-agency discussion on national security intelligence.

As expressed above, undertakings providing public communications networks or publicly available communications services in the State are required to take a risk based approach to ensure the resilience of the networks and services they provide. However, there is currently no formal mechanism by which relevant national security intelligence can be shared with providers. If they are unaware of risks based on national security intelligence, providers will be unable to take appropriate mitigation measures, either within the networks and services they provide or organisationally, to address such risks.

Goals

As set out earlier in this submission, publicly available communications networks and services play, and will continue to play, a significant role in Ireland's economic development and in its national security. The complexity of and the reliance on the technologies used to deliver those networks and services to the businesses and the public, increases the vulnerability to the resilience and security of those networks and services.

As no one Government Department or agency has full responsibility for national security, an all of Government approach to National Security is prudent. With the growing reliance of all sectors of the economy on telecommunications services and networks, there is the potential that actions taken by ComReg may have wider implications, e.g., foreign direct investment, foreign policy, etc.

To address this, ComReg proposes two goals for consideration as part of the National Security Strategy:

- *Goal 1: Secure telecommunications networks and services*
  It is imperative that current telecommunications and future networks and services, are secure given that telecommunications networks and services underpin essential socio-economic activity within the State. Without having access to national security intelligence risks, it is not possible to achieve the goal of secure telecommunications network and services within the State.

- *Goal 2: Inter-agency discussion and cooperation on national security intelligence*
  Telecommunications networks and services are essential to socio-economic activity within the State, with access to secure telecommunications networks and services being vital to citizens and businesses alike, e.g., banking, transport, health, utilities. The different sector agencies need to be able to bring their perspectives to bear on national security intelligence and cooperate on matters of national security, including to avoid taking actions which might compromise National Security.

Strategy and capacity

ComReg is of the view that a whole of Government approach to National Security is an appropriate strategy to pursue. It is important that National Security is underpinned by a comprehensive strategy,

An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

ComReg proposes that the following are important considerations in the formation and implementation of such a strategy:

- *Resourcing of the National Security Assessment Centre:* the National Security Assessment Centre will be providing a much needed service to the State (both citizens and State agencies), to do so will require the appropriate budget to:
    - attract and retain the necessary expertise into the organisation;
    - perform its functions in an effective manner; and
    - be in a position to fund its activities.
- *Sharing of national security intelligence among State Agencies:* establish a mechanism to share and/or access national security intelligence in a controlled way, particularly among State agencies. At a minimum, this could be achieved through a security clearance framework;
- *Inter-agency discussion and cooperation on national security intelligence matters:* facilitate inter-agency discussion and cooperation on national security intelligence matters. Given the interplay between State agencies and departments, national security will benefit from the combination of different perspectives on national security intelligence. This will initially require a controlled means to give access to national security intelligence, through a security clearance framework; and
- *Sharing of relevant national security intelligence with providers of public communications networks and publicly available communications services:* develop a means by which controlled access to relevant national security intelligence can be made available to providers of public communications networks and publicly available communications services in the State. ComReg can assist with the development of such process with the National Security Assessment Centre;

Although national security is a specialised area and is not within ComReg's competence, however, ComReg views a National Security Strategy as a complementary framework to its role with regard to the resilience and security of electronic communications networks and services in Ireland. Further to this, as access to secure telecommunications networks and services is vital to the State, its citizens and the economy, ComReg is fully willing to play its role in relation to national security.

Yours sincerely

p.p. **George Merrigan**
Director, Market Framework
Commission for Communications Regulation