The introduction of 5G networking technology represents a major shift in realising many advanced applications, providing the prospect of smart, near real time immersive experiences, low latency processing and the potential to improve coverage of poorly served areas. The uplift in capability that this brings can be translated into many diverse growth areas.

By improving the methods of integrating private networks and allowing them to become commonplace, helps to generate new revenue streams. This will mean that many more Small and Medium Enterprises (SME's) can benefit from a 5G installation within their premises. With an estimated 5.6 million SMEs in the UK, there is a substantial business opportunity, with private networks estimated to represent a growing market worth circa £5.5bn globally by 2027. The DCMS funded 5G DRIVE project is intended to capitalise on this opportunity, allowing diversified RAN handsets to access services provided by different participating vendors. WMG researchers are working as part of an industry consortium consisting of Cisco, ORI, Virgin Media O2 and WaveMobile to deliver on this opportunity at scale.

Increasing both the range of services and widening the types of participants involved in consuming these services is not without risk. The Secure Cyber Systems Research Group (SCSRG) led by Professor Carsten Maple at WMG have been involved since the early stages of the project to design security into the system, to provide increased accountability, oversight, trustworthiness and resilience into these networks that span both public mobile networks and private, enterprise owned, networks. The key to delivering 5G services is in providing intelligent message relay via Security Edge Protection Proxy (SEPP) capabilities to the network operator and thus protecting potentially sensitive interactions between customers and services.

The approach taken involves research into both the static and dynamic nature of cyber security in complex routing networks where ownership is varied, and security cannot be guaranteed. To counteract the potential problems these networks present, WMG researchers are undertaking investigations to identify threats to the security and privacy of the 5G network deployed in the project, with an assessment of the lightweight encryption algorithms that can be applied to protect the confidentiality and integrity of the messages being passed. A structured programme of work has yielded insights into how best to manage and model the potential adversarial threats to the system prior to implementation.

The outcomes from the project will help to accelerate the growth and uptake of advanced 5G services in a secure and reliable manner, contributing knowledge into the management, scalability, and ongoing sustainability of these fundamental services in the development of industrial strategy and product development.

For more information about this area of research, please visit the following links: https://warwick.ac.uk/fac/sci/wmg/research/digital/csc/

https://warwick.ac.uk/fac/sci/wmg/research/transformation/securecybersystems/