What does the UK need to do to pursue its spectrum resilience objectives?

A paper prepared by QinetiQ for the

UK Spectrum Policy Forum

January 2018

uk spectrum policy forum

About the UK Spectrum Policy Forum

Launched at the request of Government, the UK Spectrum Policy Forum is the industry sounding board to Government and Ofcom on future spectrum management and regulatory policy with a view to maximising the benefits of spectrum for the UK. The Forum is open to all organisations with an interest in using spectrum and already has over 150 member organisations. A Steering Board performs the important function of ensuring the proper prioritisation and resourcing of our work.

The current members of the Steering Board are:

- Airbus Defence and Space
- Avanti
- BT
- Department for Digital, Culture Media & Sport (DCMS)
- Digital UK
- Huawei
- Inmarsat
- Ofcom
- Plum Consulting
- QinetiQ
- Qualcomm
- Real Wireless
- Sky
- Telefonica
- Three
- Vodafone

About techUK

techUK facilitates the UK Spectrum Policy Forum. It represents the companies and technologies that are defining today the world we will live in tomorrow. More than 950 companies are members of techUK. Collectively they employ approximately 800,000 people, about half of all technology sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups.

What does the UK need to do to pursue its spectrum resilience objectives?

Summary

Radio spectrum access is critical, underpins the UK's economy and provides significant social value through the range of applications it supports. It is, therefore, part of the UK's (soft) infrastructure and the access to it should be resilient and appropriate spectrum protection measures should be implemented by businesses and users. It is UK Government policy to have resilience in its Critical National Infrastructure, however, as spectrum access is pervasive, there is also a **need to ensure that other key systems and services, in an increasingly integrated and interdependent society, are resilient**.

This white paper, based on the outcomes of two UK Spectrum Policy Forum (SPF) workshops, first outlines the broad need for resilient systems and provides two examples that illustrate the potential ripple or cascade effects that disruptive effects could cause. These demonstrate the need to conduct system level testing to ensure that unexpected (ripple or cascade) effects can be understood and mitigated.

Traditionally cyber security is described as an information management problem. However, as the digital economy is underpinned by spectrum access, **cyber security must include both information security and spectrum (electromagnetic) security**. This latter security could be termed cyber-spectrum security. Disruptions, via spectrum denial, have been reported for a wide range of systems. It is predicted, however, that these disruptions will increase due to a range of factors such as the easy availability of complex technology and the increasing interconnectivity of radio systems used to provide complex services. As the societal reliance on spectrum increases, appropriate cyber-spectrum security measures are needed.

To develop resilient systems an integrated strategy is required and cyber-spectrum measures must make their own contribution to the integrated approach. Unless appropriate cyber-spectrum protection measures are taken, spectrum denial or interference could be an easy axis to maximise disruptive effects.

A key element in developing resilient system is user-awareness. To enable users to integrate cyber-spectrum plans with their information cyber security plans a number of recommendations are made. These include; users being able to conduct regular, systems level spectrum-stress tests in operational environments to understand their risk; UK Governments Common Cyber Effects document being upgraded to include cyber-spectrum effects; increasing consumer choice and raising awareness by radio system and service providers creating Gold, Silver and Bronze spectrum resilience frameworks; and the effective management of over the counter interference and jamming systems.

The need for resilient systems and systems level testing

The UK Government's official definition of Critical National Infrastructure (CNI) is defined as: "*those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends*". The 13 national infrastructure sectors[1] are;

• Chemicals • Civil Nuclear • Communications • Defence • Emergency Services	• Energy • Finance • Food • Government	• Health • Space • Transport • Water

CNI must be protected against disruptive events. A disruptive event could be a natural occurrence, such as a space weather event disrupting satellites, or a human intervention event such as a criminal or terrorist incident disrupting food, energy, water supplies etc.

In a highly integrated society, even a small disruptive event could result in significant un-expected consequences.

In a highly integrated and interdependent society a small disruptive event could ripple out and cause significant un-expected consequences. Examples of such ripple/cascade effects include:

- the recent British Airways power[2] failure to the data centre not only resulted in disruption to the data-centre itself but also to thousands of passengers around the world;
- the recent NHS information-cyber attack, not only disrupted hospitals computers and theatre operations but also disrupted GP surgeries[3];

The above examples demonstrate that to absorb or mitigate the effects of a disruptive event it **is important to conduct system level testing** to fully understand the ripple/cascade effects and develop the right mitigation strategies.

In addition to the above, there is **increasing concern about the availability of highly complex technology that could be used maliciously for non CNI services**. For example:

Highly complex disruptive technology is widely accessible for malicious purposes

- technically complex Un-attended Air Vehicles (UAVs) are now easily available off the shelf and used by criminals to deliver drugs and mobile phones to prisons[4].
- off the shelf higher strength lasers are increasingly used maliciously. These are used to dazzle people and around 1,500 aviation incidents and 85 rail incidents a year[5] have been reported.

[1] http://www.cpni.gov.uk/about/cni/
[2] http://www.bbc.co.uk/news/business-40159202
[3] http://www.bbc.co.uk/news/uk-39918426
[4] http://www.telegraph.co.uk/news/uknews/law-and-order/12170213/Drones-used-to-smuggle-drugs-and-mobile-phones-into-prisons-at-rate-of-twice-a-month.html

As society and the economy become progressively integrated, interdependent and more reliant on high technology, the need for these high technology systems to be ever more resilient will be crucial.

Relevance of resilience to spectrum

Spectrum access to the UK is essential for a wide variety of services and applications. The UK Spectrum Usage and Demand[6] study has highlighted the diverse and integrated nature of the usage of spectrum to underpin the UK economy. The spectrum used by radio systems ranges from a few kHz to many GHz and is accessed via a variety of regulatory regimes. These range from exclusive licenced access to licence exempt usage. **Due to the economic and social importance of spectrum, spectrum can be categorised as part of the UK's soft infrastructure**.

image from 5g.co.uk

To increase UK economic growth, the UK's strategic spectrum-vision is to double its annual contribution to the economy from a base of over £50 billion a year by 2025. This growth is likely to be achieved by **increased spectrum usage through new applications** which may be **integrated and interconnected** such as; Smart Energy, Smart Cities, Healthcare, Smart Agriculture, Autonomous vehicles, Autonomous manufacturing, business to business services, Internet of Things (IoT) etc.

New integrated and interconnected application such as those needed for smart cities, autonomous vehicles and those being promised by 5G and technologies for Internet of Things (IoT) should be appropriately resilient

As spectrum is a part of the soft infrastructure and as new integrated and interconnected radio systems are critical to the UK, they must be appropriately spectrum-resilient if they are to contribute to a sustainable and secure economy.

Cyber and spectrum threats

The UK is one of the world's leading digital nations[7] and much of the UK's prosperity depends on our ability to secure our technology, data and networks from the many threats we face. However, information-cyber attacks are growing more frequent, sophisticated and damaging when they succeed.

Much of the UK's prosperity depends on our ability to secure our technology

[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/637087/Call_for_Evidence_Lasers_PDF.pdf
[6] https://www.techuk.org/insights/reports/item/3773-uk-spectrum-usage-demand-first-edition
[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

In the UK cyber security strategy, **'cyber security' refers to the protection of information systems** (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access intentionally or accidentally[7].

Information-cyber attacks are attacks that aim to compromise or damage computer networks via:

- jamming,
- spoofing and
- hacking

These traditional cyber effects, may be enacted by[7]; Cyber criminals (for fraud, theft and extortion purposes), States or be state-sponsored (to gain political, technological and strategic advantage), Terrorists (to attract media attention and intimidate their victims), Hacktivists in response to perceived grievances, and 'Script Kiddies' (i.e. less skilled individuals using sophisticated programmes developed by others). It is interesting to note that in the recent government document[8] "*The Key Principles of Cyber Security for Connected and Automated Vehicles*", the emphasis is on security of information and not spectrum-security.

A denial of spectrum access is equivalent to a traditional Cyber denial of service attack

The **denial of spectrum access**, through jamming, spoofing or hacking, either accidentally or intentionally, **can result in similar effects** as **information-cyber denial of service** attacks. For example, **cyber-spectrum attacks** in the space domain[9] can include jamming, spoofing and hacking attacks on communication networks; attacks targeting control systems or mission packages; and attacks on the ground infrastructure such as satellite control centres.

Cyber security must encompass both the information and electromagnetics (spectrum)

As spectrum and information-cyber activities are interdependent and as criminals, terrorists, hackers may use both spectrum and cyberspace for malicious purposes the term **cyber security should encompass both information and spectrum (electromagnetics) effects** (i.e. Cyber-Spectrum activities).

Where have spectrum disruptions occurred

The question arises of where have cyber-spectrum disruptions occurred?

An investigation of the open literature highlights that spectrum-disruptions have occurred to many systems across a number of frequencies.

Examples include:

[8] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/624302/cyber-security-connected-automated-vehicles-key-principles.pdf

[9] Space the Final Frontier for Cybersecurity, David Livingstone and Patricia Lewis, The Royal Institute of International Affairs Chatham House, International Security Department, September 2016.

- in multiple European cities (e.g. Berlin) criminals used GSM-Jammers to disable the security system of limousines[10];
- in London, UK, a city bank was the target of a blackmail attempt where the use of EM disruptors was threatened to be used against the banks IT-system[11];
- in St. Petersburg, Russia, a criminal robbed a jewellery store by defeating the alarm system with a repetitive RF generator. "It's manufacture was no more complicated than assembling home microwave ovens"[12];
- GSM-R, part of the European Train Management System, is an adaptation of the GSM mobile telephone system standard. As some of the data is safety critical, the train must stop if the GSM-R connection is lost. Compact battery powered jammers can be purchased online for GSM systems and it is likely they can be successfully operated from within the train[13];
- the number of interferences, which could stop trains running, reported on GSM-R increased to the point that Finland dropped GSM-R in favour of a domestic radio system due to Interference[14];
- interference from a 5GHz disabled Dynamic Frequency Selection mechanism[15] resulted in interferences to meteorological radars;
- ground based interference causing interference to meteorological satellites resulting in a loss in satellite capabilities[16,17] ;
- a survey carried out in 2013 by the Satellite Interference Reduction Group (iRG) and Newtec found that 93 percent of the almost 500 respondents suffered from satellite interference at least once a year[18];
- jammers that can stop road vehicles by causing interference to the electronic engine management system[19] are openly advertised;
- mobile and Wi-Fi jammers, ranging from £60- 178 are available over the internet[20] ;
- GPS jamming product caused major disruptions at Newark Airport in New Jersey as it interfered with a system to "increase airport capacity, decrease air traffic noise, and reduce weather-related delays". The airport system used GPS as an underpinning technology[21];

Mobile, Wi-Fi and GPS jammers are openly available over the internet

[10] Sabath F, "What can be learned from documented Intentional Electromagnetic Interference (IEMI) attacks". General Assembly and Scientific Symposium, 2011 XXXth URSI
[11] Hoad, R., & Sutherland, I. (2007), "The forensic utility on detecting disruptive electromagnetic interference". 7th European Conference on Information Warfare and Security": ECIW2008, 77-87
[12] The Threat Of Radio Frequency Weapons To Critical Infrastructure Facilities. United States Department of Homeland Security (2005).
[13] Dawson, J. F, Intentional Electromagnetic Interference Effects in Cyber-Physical Systems. Proceedings of EMC UK 2015. EMC UK 2015, 06-07 Oct 2015
[14] http://www.railwaygazette.com/news/infrastructure/single-view/view/finland-to-drop-gsm-r-in-favour-of-domestic-radio-system.html
[15] ECC Report 192, "The Current Status of DFS (Dynamic Frequency Selection) In the 5 GHz frequency range". Annex 2 amended 13 Februrary 2015
[16] Y. H. Kerr, P. Richaume; et al, "SMOS AND RFI: A LONG STORY"; URSI GASS Montreal, Canada Aug. 2017, –n
[17] Misra, S, Matthaeis, P "Passive Remote Sensing and Radio Frequency Interference (RFI): An Overview of Spectrum Allocations and RFI Management Algorithms", IEEE Geoscience and remote sensing magazine June 2014.
[18] The fight against interference; http://www.satelliteevolutiongroup.com/articles/Satellite-interference.pdf
[19] http://www.diehl.com/fileadmin/diehl-defence/user_upload/flyer/HPEMcarStop_e_2017.pdf
[20] http://www.jammer4uk.com/cell-phone-jammer-c-2.html
[21] https://www.cnet.com/uk/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport

- the risk of cyber attacks (i.e. jamming) targeting ships has become so serious that alternative radio based navigation systems are being considered[22];
- in June 2016 a large number of UHF radio based telemetry and telecontrol systems in the UK started to receive interference which severely impacted their operation[23];
- car theft is gaining proliferation in the UK as more criminals are using radio transmitters to perform 'relay' car hacks.[24]

These incidences illustrate **the wide range of spectrum applications that can be disrupted**. Any one of these spectrum disruptions could significantly impact the economic and social value that spectrum provides. To make spectrum stakeholders (users, technologists, policy makers etc.) aware of common electromagnetic cyber threats, spectrum users should be encouraged by government to report spectrum attacks and a document should be published illustrating case studies of attacks. Electromagnetic attacks (cyber-spectrum) should also be referenced within the Common Cyber Attacks paper[25].

Risks drivers to future denial or disruption of spectrum access

The question arises, "*Is spectrum disruption likely to get worse or less in the future*?"

Amongst stakeholders there is a consensus of increasing concern of the future ability to cause disruptive impacts intentionally or accidental using the spectrum. These risks arise from a combination of effects and drivers such as:

- increased demand and reliance on spectrum for all land, sea, air and space applications, means that a disruptive cyber-spectrum event may disrupt multiple systems and result in unintentional consequences;
- the increasing availability of open source spectrum design information;
- the availability of highly reconfigurable, complex, cost effective technologies (e.g. software defined radios) to malicious users;
- deployment of cost effective licence exempt devices, which can be easily disrupted, in key applications (e.g. health, transport, emergency services);
- civil systems potentially being more prone to disruption as interference margins are related to system cost and size;
- increased integration and interconnectivity of applications and services (e.g. Internet of Things, IoT) where a disruption on one system could cause a ripple/cascade effect and result in disruptions to other connected systems;
- increased automation (e.g. driverless vehicles and platforms) using information from wireless systems;
- users being unaware of their reliance on wireless technologies because spectrum access is hidden and become embedded in their system;

[22] https://uk.reuters.com/article/us-shipping-gps-cyber-idUKKBN1AN0HT
[23] Grilli. A, "Report into interference into UK telemetry and control systems on 5 & 6 June 2016". JRC private communication.
[24] https://www.express.co.uk/life-style/cars/885216/relay-car-theft-keyless-entry-advice-faraday-cage
[25] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf

- increasingly sophisticated adversaries (criminals and terrorists) with easily available complex spectrum-technologies;
- the need to be spectrum efficient which minimises spectrum band diversity,
- the increasing need for resilient wireless connectivity for cloud services;
- increased urbanisation where a disruptive event could impact many systems and users;
- open availability of jammers (e.g. via the internet);
- many businesses and users may not fully understand the business impact that may be caused through a disruptive spectrum event;
- a disrupting spectrum event may be difficult to attribute (e.g. geo-locating a jammer in a city environment could take many hours or days) and hence conducted anonymously;
- in the defence and security arena the interdependence of Cyber and Electromagnetic security is well understood. In the commercial sector electromagnetic (spectrum) security does not have the same profile at board level as information security;
- both localised (e.g. GPS jamming) and geographically widespread (e.g. satellite interference) effects can be caused by disrupting spectrum access.

It is concluded from the above factors that **the impact and risk of malicious or un-intentional interference is likely to increase** and result in potentially significant economic and societal losses.

In the space domain economic impacts alone could range from <£1M to >£100m and the economic loss of GPS (e.g. via spoofing and jamming) has been estimated to be many millions of pounds[26]. To highlight the implications of spectrum disruptions to other services and applications the economic impact of the loss of spectrum should be further investigated.

To minimise the easy availability of jammers, legislation should be reviewed to assess if additional consumer protection is required as is being considered with high power laser sources[27].

Achieving Resilience

Resilience (e.g. for infrastructures) is achieved[28] through an integrated strategy comprising a combination of; resistance (which is focused on providing protection), reliability (i.e. components that are inherently designed to be reliable under a range of conditions), response and recovery (ability to recover from the disruptive events) and redundancy (availability of backups). The contribution of each element will be related to its cost effectiveness and the

[26] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf
[27] https://www.gov.uk/government/consultations/laser-pointers-call-for-evidence
[28] Section A: Introduction, Definitions and Principles of Infrastructure Resilience, Cabinet Office

anticipated level of risk. Risk can broadly be defined as the likelihood that a disrupting event will occur combined with its impact.

As many applications critical to the UK economy rely on information transmitted using the radio spectrum, spectrum disruption must be considered alongside traditional (information) Cyber effects. Cyber-spectrum protection measures, therefore, should contribute to an overall integrated resilience strategy.

Lloyds of London say that companies should ensure their systems are rigorously tested and externally validated before they can feel confident about their level of preparedness. Even then, it's essential they remain constantly vigilant and regularly update their plans as new threats emerge[29].

As cyber-spectrum events are linked to traditional information cyber effects, the need to conduct **system level testing of both the information and cyber-spectrum effects is critical** if the full disruptive effects are to be understood and mitigated. Spectrum users or authorise bodies, therefore, should be able to conduct Spectrum Stress Tests in realistic operational environments to examine the vulnerability and develop mitigations. These mitigations could include; procedures and policies, additional technology such as monitoring systems to detect anomalous behaviours and provide an early warning system to potential attacks, access to additional spectrum for diversity, dynamic spectrum access, or even a minimum wireless service obligation level to maintain a minimum level of wireless connectivity.

To aid consumer choice, spectrum resilience accreditation levels (e.g. Gold, Silver, Bronze) should be developed. These could be developed for the radio application the system, or for the facilities that use spectrum.

Recommendations

Based on the workshops held by the SPF, the following strategic recommendation is made;

Government departments, private sector service providers and spectrum users' ***should conduct regular "spectrum stress tests" to understand their spectrum-resilience risks and develop appropriate mitigation techniques.***

Spectrum users should be able to conduct regular system level spectrum stress tests on operational systems so that appropriate mitigations can be put in

To achieve this, the Spectrum Policy Forum should ***develop a Framework guidance document on achieving spectrum resilience.***

To underpin the spectrum resilience requirements Government departments (e.g. DCMS, Dept for Transport, Department for Business, Energy & Industrial Strategy) should investigate if spectrum (electromagnetic) disruptions should be included in the National Risk Register[30].

[29] Facing the cyber risk challenge - A report by Lloyd's 20 Sept. 2016

[30] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf

To support the broader Cyber-Spectrum Security agenda and the development of a Framework document it is recommended that:

Recommendation	Comment
1. DCMS and users should develop Policies and procedures that enable spectrum users or authorised bodies to conduct regular system level "Spectrum Stress Tests" (e.g. jamming, spoofing etc.) in operational environments such as; a city, factory, roadsides, remote outdoor location etc.	This will enable users or authorised bodies to conduct spectrum stress testing using illustrative (authorised) interference sources in realistic environments on operational systems. This will inform users of their spectrum risks and enable them to develop appropriate mitigations.
2. Government should encourage the reporting of spectrum attacks and a document should be published illustrating case studies of attacks. Electromagnetic attacks should also be referenced within the Common Cyber Attacks[31] paper produced by the National Cyber Security Centre.	Highlighting spectrum attacks within the Common Cyber Attacks will highlight the interdependence of spectrum and information and inform a wide range of stakeholders. Encouraging reporting will contribute to the awareness and a case studies document will highlight the impact.
3. Spectrum stakeholders should investigate the economic impact of the loss of spectrum to their applications and services.	The economic impact of the loss of spectrum will underline the need for resilience and promote the risk at board level and support an entry into the risk register.
4. Government should continue to deal with spectrum threats and consider what additional legislation may be required to protect consumers and business by restricting the sale of RF jammers.	This will protect users of spectrum devices and the consultation could be similar to that being pursued for high power lasers[32].
5. To provide consumer choice, technologists, industry and businesses should design resilient equipment and services (e.g. 5G, IoT, autonomous applications) and consider the concept of different spectrum resilience accreditation levels (Gold, silver, Bronze) for technology and services. The accreditation could be based on the mitigations used e.g. monitoring systems to detect anomalous spectrum behaviours, access to additional spectrum for diversity, or even access to a minimum wireless service to maintain a minimum level of wireless connectivity.	This will ensure that resilience is available to consumers and is an integral part of our future inter-connected and interdependent society. Resilience guidelines/standards could be applied to physical spaces e.g. spectrum resilient building as well as radio systems.

[31] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf
[32] https://www.gov.uk/government/consultations/laser-pointers-call-for-evidence