Contents:

1-Introduction

1.1 This Response concentrates on digital issues relevant to revision of the Official Secrets Act (OSA) and related legislation where the professional input of **The BCS - The Chartered Institute for IT** can add value, in particular, on developments in information technology (IT) and in information and cyber security. This Response adopts such an approach with the view to offer the legal community a better understanding of these developments in terms of background information or for potential application. The main body of the Response thus does not focus on line-by-line analysis on where to insert these digital concepts nor provides interpretations of these concepts in terms of legislative sections and phrasing. Appendix C, however, provides considered thinking on some sections selected from among the List of Consultation Questions and Provisional Conclusions provided by the Law Commission.

1.2 This Response is from a Working Party (Appendix A) set up by the Law Specialist Group (SG) at The BCS – The Chartered Institute for IT (formerly the British Computer Society). It considers the Law Commission request for comments on the document 'Protecting Official Data' and via dialogue with Professor David Ormerod during his visit to the BSC Law SG's first meeting on 8 March 2017, to discuss the document and request. The Working Party met again on 12 April 2017, to discuss inputs and preliminary conclusions, with further email discussion to finalise the Response.

1.3 With so much information on cyber and information security issues in the open / public domain, awareness of which has been raised by activities such as the Snowden affair, there is an onus on government entities particularly those responsible for national security and public safety, to see what is in the public or open domain. This can include consideration of or implies the following to do:

- Contribute to their analysis. Towards this end, not only has the cyber security industry been looking at technically oriented vulnerabilities, but also security research institutes and social media are increasingly publishing information, with additional value of providing political, cultural and other context not normally associated with the narrow technical focus on cyber vulnerability and security analysis (e.g. see security data analytics of Palantir.com; IISS.org weekly cyber incident report).

- With (so-called) open source intelligence (OSINT), government entities also have the onus to re-evaluate and reduce what information (e.g. operational, actionable) is actually to be categorized as classified, with staff hiring and vetting policies to be revised and monitored accordingly.

- Understanding context wider than technical will also enrich risk analysis of any enterprise. Risk analysis in the business world has traditionally focused on financial risk, but controls and standards are increasingly requiring boards to consider risk more widely. These include ISO risk management standards (see Appendix B) which can facilitate and improve existing corporate governance guidelines and requirements (e.g. Sarbanes-Oxley for U.S. corporations and companies listed on stock exchange).

- The Security and Risk Management Domain (1) of the CISSP (Certified Information Systems Security Professional, revised 2015) highlights the interrelationship between information and cyber security controls within a wider risk management framework encompassing strategic, financial, organisation, technology, operations, legal/regulatory concerns. These are complementary to existing corporate governance requirements.

- With the large increase of cyber security information in the open / public domain (and with the implementation of General Data Protection Requirements (GDPR) by May 2018), company directors can no longer plead ignorance of cyber and information security issues to minimise their liabilities. This implies that costs of protection, mitigation, business continuity and other areas, are to be covered by enterprises as they are risks for which they can now be reasonably expected to know, especially when it is well-known that many vulnerabilities remain repeatedly unaddressed (e.g. Open Web Application Security Project's (OWASP) annual top ten web-based application security flaws and how to mitigate them.) When these and other commonly repeated flaws are addressed and reduced, e.g. in the public and commercial sectors, it would seem that government security entities can focus more on threat (State) actor cyber 'attacks' vs 'incidents' (*incidents* being a neutral term before intent and attribution are determined).

2-General Comments and Suggestions

- The revised OSA/related legislation might require each government department to nominate or designate a person who understands both the work of the department and how the IT systems operate to support that work (in addition to there already being a person responsible for supporting information security measures).

- Such a person might also cooperate with the Data Protection Officer, required to be designated by the GDPR, such that information security and privacy can be considered simultaneously for simplification and to minimise areas of possible conflict.

- Her Majesty's Government also has a consultation for information that might be derogated from the GDPR requirements. This implies possible official secret information among other factors that might affect the process and or content of the revised OSA.

- Good Corporate Governance practices can be considered for adoption in government not only to more effectively manage government operations but also for staff to be aware of commercial and business culture, development and use of new information technologies and types of information arising. 'Codes of Practice' or good practices and standards to meet new challenges and their mitigation, already exist. These include standards such as the ISO 31000-2009 family on risk management; guidelines of the Security and Risk Management Domain (1) of the Certified Information Systems Security Professional (CISSP); and a range of security standards including ISO 27001 (Information Security), ISO 27010 (Critical National Infrastructure), ISO 27017 (Cloud Services), ISO/IEC 27013 (Information Tchnology – Security Techniques), ISO 20,000-1 (IT Services Management and Integrated Implementation), ISO 27018 (Personally Identifiable Information), ISO 27032 (Cyber Security Guidelines), and ISO 27552 (Privacy Management).

- The Working Party also recommends an independent advisory IT Review Body or standing group comprising a combination of IT, commercial data, information and cyber security as well as legal specialists, appointed to identify relevant standards, regulations and good practices as well as methods of maintaining and monitoring their implementation and dispute resolution. The advisory group would not perform these functions, but serve as an external resource for guidance as needed, and conduct regular meetings to provide opportunity to share practices, experiences and lessons learned, and lessons to be learned, as well as discuss future challenges, to help guide, elaborate or finalise issues in the realms of data security in the fast pace growth of IT and technological developments and applications.

- In addition to civil service training, hiring and vetting policies might be reviewed as well as implementation of policies and procedures versus policing (but that is possibly beyond the scope of the revised OSA).

2.1 Comment

The below are comments on terms to serve as guidance to facilitate understanding and guidance for legal practitioners and related professionals.

- **Remote Location**

  This definition might be wide ranging taking into account the transnational nature of data as to where it is created, processed, transmitted and/or stored, whether in a single country and/ or in 'clouds' located globally. Additionally, civil servants can have awareness raising or training to address the following concerns of location, common within and outside government:

  a) Creation of dynamic audit logs and 'after' data artefacts is often sporadic across departments;

b) Asset registers often require maintenance and updating when assets are not only acquired but also relocated and disposed;
c) System protecting and vulnerability management practices are needed.

- **Whistleblowing**

  A new 'Whistleblowing Protocol' is suggested whereby the electronic equivalent of a 'Dead Letter Box' is provided to protect the identity of both the Source and the Recipient, with an overriding 'non-blame' culture to be fostered and encouraged.

- **Criminal Intent**

a) *In the absence of criminal intent*, there can be a consideration (in any replacement of the OSA) that a crown servant may offer as a defence, that preparation of material having been exposed to the public domain had been derived with no malicious intent by data analytics of information already in the public domain (provided the method is prescribed and repeatable).

b) Many companies in the cyber security sector monitor their own unclassified sources of data and systems in order to create 'intelligence reports' (here meaning not for the government, in which case intelligence is in quotes as is not derived by and/or for government) on vulnerabilities and the threat environment. These reports are offered as a service to many clients, some of whom may fall under the broad remit of 'foreign entities' under the proposed changes. It would be detrimental to the British cyber security industry if this activity were curtailed. The revised act may criminalise legitimate security research necessary to protect organisations from criminal or foreign nation State actors. Such dissemination, however, might also indirectly foster a form of transparency that could contribute to diplomacy between governments in resolving cyber 'incidents' before they are labelled as 'attack'.

c) Criminal Intent in 'digital' matters may need different levels of the 'Burden of Proof' (e.g. beyond reasonable doubt, balance of probability).

d) There might be needed a category of 'Digital offences' under which crimes might be classified and prescribed as solely 'digital' as distinct from crimes traditionally offline also being conducted online.

e) Proof of Evidence, where machine learned software inadvertently has '*unintended consequences*' - it is suggested to have causal activity and each case to be looked at on its own merits.

f) The cyber security industry has an obligation to protect its clients (including those abroad) from 'attacks', some of which might be conducted by the UK Government.

g) The broad definition of a foreign power to which intelligence may not be divulged includes many legitimate non-UK organisations which may be clients of a cyber security provider.

h) The proposal appears to subject unclassified proprietary data sources to secrecy provisions. Should the status of any proprietary data be considered; is there a distinction between sources of data and the data itself.

- **Code of Practice**

  Good governance to include companies which use and manage outsourced work, consultants, supply-chain and temporary workforce, to also demonstrate compliance and obligations similar to government employers.

  Departments should have in place methods to check their own departmental compliance with the code or such standards that are in place, and share good practice among departments. As a complement, however, it is suggested that an independent advisory body be created as mentioned above.

  To consider whether monitoring 'Public interest' concerns are to be part of 'Code of Practice'?

- **The Trend towards Commercialising Official Data**

  What protection(s) and provisions will be made of and for official data that is commercialised for financial gain compared to officially-held data shared (non-commercially) for public benefit? What is the application of the GDPR on official data, taking into account the results of another consultation on derogations for GDPR as applied to government data.

- **Intellectual Property**

  It was noted that 'Intellectual Property' of such possible 'commercialised' official data was not included in the consultation.

3-Terms for Consideration

Suggestions for defining or considering some terminology include the following;

- **Non-Deterministic Data Processing**

  Code that is capable of re-configuring its operational paths in accordance with changing conditions related in the data it is processing without human intervention, which could include e.g. machine learning. Such examples are or rely on Complexity Theory, e.g. Decision Support, Expert Systems, Artificial Intelligence (not to be confused with self-writing).

- **Software that is 'self-writing'**

  Code that will reconfigure according to changing conditions without human intervention**.** This could include examples such as when two 'machine learning' computers communicate with each other and inadvertently

conduct an operation that programmers had not thought of (see the *Moiri* report about public perceptions published alongside *Machine Learning*, Report of The Royal Society report, April 2017, https://royalsociety.org/topics-policy/projects/machine-learning).

- **Intent**
  Showing earnest and eager attention to the achievement of some goal whether or not it is 'attempted' and /or failed to have intended results.

- **Anonymous**
  Being unidentifiable by name or other nomenclature e.g an alias or avatar.

- **Avatar**
  Manifestation or embodiment of some alias, pseudonym or entity designed for deception or disguise.

- **Public Domain**
  Conceptual area or territory predominantly characterised by public citizens, groups and organisations, or is its focus meant to be only on individuals of a State or States.

- **Artificial Intelligence**
  The science and theory underpinning the development of capabilities normally requiring the human qualities of intelligence / intellect.

- **Machine Learning**
  Machine learning is a form of artificial intelligence that allows computer systems to carry out complex processes by learning from examples, data, and experience, rather than following pre-programmed rules. (*Machine Learning*, Report of The Royal Society, April 2017 https://royalsociety.org/topics-policy/projects/machine-learning).

- **Neural Networks**
  Neural networks are an approach to machine learning in which layers of computational units are connected to each other in a way that is inspired by connections between neurons in the brain. (*Machine Learning,* Report of The Royal Society, April 2017, p. 111, via https://royalsociety.org/topics-policy/projects/machine-learning). An example could be computing capability emergent from design based around 'pattern processing' and recognition.

- **Reputation**
  Generally held beliefs about a state, organisation, person or thing.

- **Anonymised Data**
  Data which has been made un-attributable, with no traceable data subject or owner or originator already in the Public Domain. This could be data 'clean' of personal details, to be non-attributable, so that such data can be used in research, medical, and other areas (perhaps analogous to the 'Chatham House Rule'?). Criminals might do the same but it seems they instead try to hide or disguise the fact of their existence, and not just 'scrub' personal details of their identity.

- **The 'Moral and Ethical' Algorithm**
  A term referred to by some persons who perceive the mathematical equation (algorithm) used in a piece of software influences or makes safety-critical or life-saving decisions, activities and/or outcomes e.g. Artificial Intelligence for use in accident avoidance decision-making in 'driverless cars', and other such automated systems.

- **BCS Glossary of Computing**
  A publication of the BCS that can be a useful source of information and guidance.

- **OWASP.org**
  Recognised for its annual top ten web-based application security flaws and how to mitigate them, most of which are repeated each year as end-users fail to correct or mitigate those most commonly occurring.

4-Appendices

Appendix A:

Contributors to the Working Party:

Overseen by Ray Long	Immediate Past President, BCS
Jennifer Dean	Chair BCS Law SG, BCS, MSc, LLB, LLM, Bar, CNA, Certs
Dr Stephen Castell	Programme Development in Law SG, BCS
Sabine McNeill	Secretary of Law SG, BCS
Dr Olivia Bosch	Committee Member of Software Practice Advancement SG, and of the DevSecOps SG, BCS
Colin Pearson	Director PPS Ltd
Nigel Young	IT Forensics
Vidya-Shankar Panchanathan	BSc(Hons) MSc, MBCS, MIAP, ISO Standards Implementer (www.management-support.org.uk)
Mazin Zeki	Liberty
Dilibe A. Aneke	
Michael Batchever	
Martin Lee	
Chiara Rustici	
David J Strudwick	MSc. (Oxon), MBCS, M.IISP

Appendix B:

Some Key ISO Standards:

ISO 27001 (Information Security)
ISO 27032 (Cyber Security Guidelines)
ISO 27552 (Privacy Management)
ISO 27017 (Cloud Services)
ISO 27018 (Personally Identifiable Information)
ISO 27010 (Critical National Infrastructure)
ISO 27014 (Governance of Information Security)
ISO 20 000-1 (IT Services Management and Integrated Implementation)
ISO 22316 (Organisational Resilience).

Appendix C:

Selected Sections for Comment

Conflict of National Interest vs Client Protection

The consultation introduces some concept of the notion of what is encompassed by espionage:
Sections
1.2 "criminalisation is limited to the unauthorised disclosure of those categories of information that have implications for the national interest."
1.3 "criminalise individuals whose purpose is to gain access to information, potentially by using covert means"

2.3 "Espionage focuses on gathering non-public information through covert means. Classified information is kept secret in the first place because its disclosure might harm national security, jeopardise the country's economic well-being or damage international relations."

One of the goals of any cybersecurity company is to research the threats which impact their customers. The majority of this research is conducted using proprietary non-public information obtained from unclassified sources.

In 2013, the secretary of defence stated that the UK was "developing a full spectrum military cyber capability, including a strike capability" https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de.

The 2016 HM Government National Cyber Security Strategy describes,
"*Through our National Offensive Cyber Programme (NOCP), we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability.*"

One of the stated goals of the strategy is to ensure that,
"*The UK is a world leader in offensive cyber capability."*

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

It is conceivable that the UK may conduct offensive cyber operations against an organisation which a cyber security company is contractually obliged to defend. Through their own endeavours with access to entirely unclassified but non-public data the company may be able to detect the 'attack'. At that point, the company would be obliged to report the existence of the attack to their client.

Many cyber security providers are proud of their capability to detect and identify the attacks of nation state actors. This research forms part of the many security publications and the services offered to clients.

It can be expected that private sector cyber security providers will be able to identify attacks undertaken by the UK (or other) government even if they are unable to provide direct attribution. In these cases, the provider will [might) be contractually obliged to report the existence of the attacks to their clients.

Being able to communicate the existence and likely attribution of attacks is a fundamental tenet of any protective cyber security organisation, but attribution is well known to be difficult to determine. Instead, in the absence of direct or definite attribution, the focus of attention of an entity suffering a cyber 'incident' (compared to an 'attack' which implies known intent and direct attribution of source) is business continuity and often reputation management.

The Proposed Nature of a Foreign Power

The consultation describes:
2.138 "This element of the offence seeks to ensure that the offence is limited to cases where there is not only knowledge or reasonable grounds to believe that the conduct might harm the interests of the United Kingdom as we have just discussed, but that the conduct might benefit a foreign power. "

We agree entirely with the consultation when it states:
2.140 "The increasing power of companies within state structures, and complex governance models, can make it difficult to determine whether an entity such as a company is acting in a private capacity or as an emanation of the state."

The consultation further describes possible classes of "foreign power" taking examples from US legislation, including:
2.141 "(1) A foreign government or any component thereof, whether or not recognised by the United States.
(3) An entity that is openly acknowledged by a foreign government or government to be directed and controlled by such foreign government or governments.
(5) A foreign based political organisation, not substantially composed of United States persons."

Communicating the presence and nature of cyber threats is an integral part of the cyber industry. In effect, this comprises a large part of the sales and marketing activity of the entire industry. It is also the manner by which the industry proves its utility.

The broad definition of the nature of a foreign power to which is it proposed to forbid the disclosure of intelligence would seem to include:

Any non-UK government,
Any non-UK public sector organisation,
Any private sector organisation part-owned by the public sector,
Any non-UK political party or lobby group.

Provisional conclusion 3 of the consultation provides that:
2.150 We have provisionally concluded that an offence should only be committed if the defendant knew or had reasonable grounds to believe his or her conduct was capable of benefiting a foreign power.
Yet many organisations encompassed by the definition may be legitimate clients of a cyber security provider. Supplying cyber technology to protect a non-UK public sector organisation against offensive cyber attacks by definition benefits the contracting organisation, which may be classified as a foreign-entity.

Cyber security providers follow the laws of the countries in which they operate. The US has clearly indicated the countries to which US based companies may not supply services. This list is clear, easy to comply with and not overly restrictive. However, the proposed definition of foreign entity is overly encompassing and would greatly hinder any cyber security company affected by the proposed law.

Consultation Question 3 asks:
2.144 Is the list of foreign entities contained in the Espionage Statutes Modernization Bill a helpful starting point in the domestic context? Do consultees have views on how it could be amended?

Perhaps taking a more prescriptive line of listing specific entities or relationships to which intelligence may not be supplied would allow organisations to apply some sort of test to potential clients to determine if they were precluded, e.g. for a prospective client: does a named individual have a major shareholding; is the client based in one of a list of precluded countries, etc.

Protecting Cyber Intelligence Research and International Relations

Cyber security is an emerging domain. Much academic research is currently being undertaken as to how nation states are using cyber issues to further their geopolitical ambitions. Part of these nation state activities is to conduct offensive cyber operations as part of the armed forces, to out-source the conducting of such activities to the private sector, or to develop a form of cyber-privateering to encourage and to direct the activities of 'patriotic hackers'.

The research of the development of such groups and the nature of their relations to nation states is vital to understanding cyber security and to provide security to the systems that the cyber security industry seeks to protect.

Publishing the findings of such research is necessary to stimulate further research and to inform organisations, including those based in the UK, of the risks that they face.

Publications such as the Mandiant's report into the activities of Chinese state directed hacking groups have been fundamental in the development of cyber security as a discipline, and informing practitioners of the threat environment (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; see also *China's Cyber Power*, by Nigel Inkster, *Adelphi* series, International Institute for Strategic Studies (IISS), May 2016).

The proposal in section 3.161 would appear to be at risk of criminalising the publication of research into state sponsored attacks for fear of being detrimental to international relations and diplomacy, though the proposal does refer to 'unauthorised' disclosure. (There are philosophical/practical reasons for transparency for security purposes but this is not for this consultaion.) This might seriously hamper the ability of cyber security provider to publish reports relating to security issues but it would be thought that a provider, contractor or other in supply chain would also be covered by the OSA.

3.161 A person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to security and intelligence, defence or international relations knowing that that disclosure is capable of damaging security and intelligence, defence or international relations.

Lawfully in the Public Domain or Widely Disseminated

Keeping secrets secret is a vital part of the operation of any organisation including a nation state. National secrets deserve to be protected by law. However, classified national systems do not have a monopoly on knowledge regarding security. Private sector organisations have developed the capability to independently observe and investigate many issues that were previously only accessible to the resources of a nation state. This is especially true in the cyber domain.

Google Earth is an excellent example of satellite images made available to the public that previously were only to the security services. Now anyone can search for the presence of military technology in North Korea for example, from their homes. While this activity would appear to fall outside the remit of the official secrets act, such information is now in the public domain, and it would be expected that security services reconsider how they safeguard their assets. There is Cold War history on how the State spoofs military assets knowing satellites were looking down, and it would be expected such camouflage and related operational security measures of military assets continue.

Private sector organisations have analogous data sources when it comes to the operation of the Internet. The Internet is primarily run and operated by the private sector, and telemetry from systems operated by private sector entities describes the nature of Internet traffic and detects cyber attacks.

These data are not necessarily available to the public, although this may be the case in certain circumstances. These data are certainly not widely disseminated; but these data are generated from non-governmental unclassified sources.

Analysis and research of these data sources generates security intelligence regarding cyber attacks without any unauthorised access to restricted data. Who then determines the truth of such data. And even if States know of a cyber 'attack' (as distinct from neutral term 'incident'), it does not mean States retaliate like-for-like; and transparency can assist diplomatic solutions; and even if there were an 'attack', the Laws of Armed Conflict (LOAC) would be expected to come into play. This is an area of ongoing debate.

Provisional conclusion 15 provides:

3.204 We provisionally conclude that a defence of prior publication should be available only if the defendant proves that the information in question was in fact already lawfully in the public domain and widely disseminated to the public.

It is suggested that a more appropriate conclusion would additionally include that the defence of prior publication should be available if the defendant can show that the information was derived from sources that are not classified, and that do not require governmental authorisation to access; and that there is not necessarily an ''and' that information is 'widely disseminated to the public' as dissemination has in past been deemed to include posting on a website.

The current provisions would seem to provide challenges or restraints on (if not outlaw) legitimate activity currently undertaken by the cyber security industry and research institutes.

Reflections on Consultation Questions and Thoughts

Thoughts 2

The generic term 'information' is too broad. The act should define the origin of the gathered or communicated information as being classified. Otherwise, the gathering of information relating to cyber attacks from non-classified, proprietary sources risks being 'outlawed', 'subject to prosecution', under the proposition. These attacks might be conducted by a hostile foreign entity, in which case the fact that they were detected assists a foreign power in refining their attack techniques. Though transparency can provide an avenue also to find diplomatic solutions, if not dealing with criminal entities.

Consultation Question 2

Yes, an offence should only be committed by someone knowingly prejudicing the interests of the State / nation security and that any gathered information is derived from classified sources. Again, otherwise the law risks prosecutions of the collection of information relating to cyber attacks conducted by nation states, or the researching of system vulnerabilities.

Consultation Question 3

The scope of the proposed definition of foreign entities is unworkable. It makes an onerous burden on any organisation conducting business outside of the UK to identify potential customers as falling under the provision of a possible 'foreign power'. Presumably the act envisages that cyber security providers must inspect the share register of potential clients and continue monitoring the share register to ensure that a foreign nation state does not become a majority shareholder through subsequent share holdings or acquisitions.

If the government is unable to maintain and publish a list of organisations to which information should not be shared, then it is unreasonable to expect that individuals or organisations to conduct the detailed, and potentially classified, research themselves.

A representative example is Huawei, a major Chinese company, which is considered by the US House Intelligence Committee as "cannot be trusted to be free of foreign state influence". A security researcher discovering vulnerabilities in Huawei equipment known to be used in the UK's critical national infrastructure may fall foul of a proposed law if the nature of the vulnerability was disclosed to the manufacturer. Since, the manufacturer could be seen as a Chinese Government controlled organisation, and the vulnerability could have a detrimental to the interests of the State.

Similarly, an organisation providing cyber security service to a Huawei subsidiary, reporting intelligence on cyber attacks launched against the subsidiary may fall foul of a proposed law by disclosing intelligence relating to attacks suspected as being attributed to the UK or an allied country to a foreign entity. It might be considered how 'intelligence' is determined, whether by, or authorised by, government compared to 'intelligence' provided by cyber security industry or related academia as a service marketed as 'intelligence.

Thoughts 3

Yes, but only if the information gathered was derived from a classified source. Again, otherwise the law risks outlawing or making subject to prosecution the collection of information relating to cyber attacks conducted by nation States, or the researching of system vulnerabilities. There has also been an evolving good practice of responsible 'vulnerability disclosure' by companies whose business is to detect software/ system vulnerabilities.

Thoughts 6

Applying broad generic terms would bring far too much information under the remit of the revised act which would outlaw much legitimate research and again risk outlawing, or subjecting to prosecution the use of much information. The proposed act should facilitate the clear distinction between information able to be used by (industry) researchers, and information subject to the revised OSA, so that it is clear when an offense is made e.g. information labelled with some sort of classification, though without risking a resurgence in classification marking that might not be needed. However, sometimes a clear distinction is not intended to be made, as it might provide parametres around which circumvention is facilitated.

Thoughts 7

The nature of 'sufficient link' is vague and poorly defined. A well-defined definition makes it clear when an offense may be committed or not. However, defining a 'sufficient link' would want to avoid the single sole source problem;

pending a burden of proof level, it would seem prosecution or defence would need some additional factors to bring to bear.

Thoughts 15

Information is either in the public domain or it is not in the public domain. There is no legal basis or test for the notion of information being 'widely disseminated to the public'. (The U.S. has had experience of considering controls on cryptographic research that began to be invented outside the traditional government domain). If information has been placed in the public domain, then it is by definition, no longer secret, even if it has never been read. This provision for being widely disseminated risks outlawing niche security research, such as on cryptography, which is vital for keeping systems secure, but whose research tends not to be be 'widely disseminated'. It may be that trade or commercial secret approach is undertaken; this approach has been noted in past to be even more stringent than what was required for 'military' security.

Consultation Question 8

The research of the development of such groups and the nature of their relations to nation States is vital to understanding cyber security and to provide security to the systems that the cyber security industry seeks to protect.

Publishing the findings of such research is necessary to stimulate further research and to inform organisations, including those based in the UK, of the risks that they face. Risking prosecution under the OSA hampers such research and acts as a break on innovative research being carried out in the UK, and that research alone could at least be exempted (e.g. some arms control treaties in effect do not disallow research for protective, prophylactic or peaceful purposes).

Appendix C.1:

CHAPTER 8

LIST OF CONSULTATION QUESTIONS AND PROVISIONAL CONCLUSIONS

CHAPTER 2: THE OFFICIAL SECRETS ACTS 1911, 1920 AND 1939

Provisional conclusion 1

a. We provisionally conclude that the inclusion of the term "enemy" has the potential to inhibit the ability to prosecute those who commit espionage. Do consultees agree? ***[Which alternative noun would be preferred? Opponent, antagonist, THREAT ACTOR…it is a view that there needs to be a satisfactorily defined term relating to hostile individual(s) (irrespective of the prevailing political conditions…war/peace etc) which is the main deficiency of 'ENEMY'.]***

Provisional conclusion 2

b. Any redrafted offence ought to have the following features:

i. Like the overwhelming majority of criminal offences, there should continue to be no restriction on who can commit the offence; *[Agreed]*

ii. The offence should be capable of being committed by someone who not only [redacted] but also by someone who obtains or gathers it. It should also continue to apply to those who approach, inspect, pass over or enter any prohibited place within the meaning of the Act. *[strongly believe the act should be extended to those who might be identifiable as providing the mechanism by which this outcome is achieved. This should include corporate responsibility, e.g. firms deliberately adopting demonstrably poor security regimes to reduce cost.]*

iii. The offence should use the generic term "information" instead of the more specific terms currently relied upon in the Act. *[the term must be properly defined to encompass the the widest possible contexts (as regards threat actors) and methods to render defense impossible.]*

c. Do consultees agree?

Consultation question 1

Should the term "safety or interests of the state", first used in the 1911 Act, remain in any new statute or be replaced with the term "national security"?

[A suggestion is to use both, as safety of the population implies also their security/ vice versa; another view is that 'National Security' would be preferable because of its alignment with other related terms and concepts such as assets constituting 'Critical National Infrastructure' which could even be categorised.]

Consultation question 2

d. Do consultees have a view on whether an individual should only commit [vs also attempt, aid and abet or finance efforts thereof – this now required in UN mandated legislation for all States?] an offence if he or she knew or had reasonable grounds to believe that his or her conduct might prejudice the safety or interests of the state / national security?

[The kind of people who are involved with sensitive official information would be fully cognizant of such grounds.]

Consultation question 3

e. Is the list of foreign entities contained in the Espionage Statutes Modernization Bill a helpful starting point in the domestic context? Do consultees have views on how it could be amended?

[DJS - Unable to comment as not possible to find the aforementioned 'list', but it might constitute a start?]

Provisional conclusion 3

f. We have provisionally concluded that an offence should only be committed if the defendant knew or had reasonable grounds to believe his or her conduct was…

See General Definitions Sect. 263 of the new Investigatory Powers Act 2016. There is some useful attempts to clarify things there.

This page intentionally left blank.