# Controlling Your Exposure: A Guide to Digital Risk and Intelligence

Digital, Data
& Technology

CYBER SECURITY
PROGRAMME

V2.0

March 2019

# Executive Summary

Digital Risk and Intelligence (DR&I) is the process of monitoring, detecting and remediating threats within the public domain, through the control of an organisation's digital footprint. This makes it harder for threat actors to plan and commit attacks, and therefore reduces the likelihood and impact of intrusions.

Government departments are progressively putting more data online, and so their digital footprints are becoming increasingly large and complex. A key objective of the National Cyber Security Strategy is to make the UK “a hard target for all forms of aggression in cyberspace”. With this in mind, DR&I is increasingly becoming something that government departments need to consider. Mitigating the threats at the earliest possible opportunity will limit the effects of attacks and reduce the overall risk to organisations.

This paper recommends how government departments can control their digital footprint through developing a DR&I capability. Before adopting these recommendations, government departments should conduct a self-assessment of their current capability using the provided Capability Maturity Model.

### Short-term recommendations at the Threat Intelligence Team level for mobilising a DR&I capability:

- Appoint a DR&I team lead, most likely from the cyber threat intelligence team, who can dedicate time to DR&I activities;
- Define the scope of the DR&I capability, and a team charter, to ensure the appropriate areas of the footprint will be focused on;
- Adopt a series of low cost, publicly available tools as Quick Wins, to easily manage the digital footprint of a government department.

### Medium-term recommendations at the Government Department level, for enabling DR&I teams:

- Commission external digital risk exposure assessments of their digital footprint at least once a year, to understand how the footprint is changing over time;
- Explore vendor trials to adopt, in order to utilise the tools and services in the market, at low cost, to make use of available capability;
- Liaise with the appropriate law enforcement agency, through the department’s legal teams, to assist in developing policies for monitoring specific public domains, as well as advising on response plans;
- Create an educational awareness campaign to encourage employees to better control their digital footprints.

## Longer-term recommendations at the cross-government function level:

- The Cabinet Office, supported by the NCA, NCSC and Government Legal Profession, should provide clear legal guidance to enable government departments to safely and lawfully monitor public domains;
- The Crown Commercial Service should provide clear, reasonable frameworks to assist departments in adopting vendor trials, and eventually procuring managed services;
- The NCSC should assess the feasibility of centralising elements of DR&I as part of Active Cyber Defence and adopting DR&I activities as part of the Cluster Security Units service offerings.

As digital footprints grow in size and complexity, we expect the risks to government departments to increase. We recommend that HM Government makes the appropriate investment and changes across cyber threat intelligence teams, departments, and cross-government functions, which will fundamentally lead to improvement in the collective security of government information and infrastructure, making HM Government a hard target for cyber-attacks.

# Table of Contents

# List of Figures

# List of Tables

# 1 Introduction

## 1.1 Background

As stated in the first line of The National Cyber Security Strategy 2016-2021 (NCSS) (1):

*"The future of the UK's security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats and equipped with the knowledge and capabilities required to maximise opportunities and manage risks."*

One of the key objectives in the NCSS is that "*The UK will be a hard target for all forms of aggression in cyberspace*". Similarly, the paper Cyber Threat Intelligence: A Guide for Decision Makers and Analysts (2) advocates a "threat-led" approach in Cyber Security. This means understanding your organisation's threat landscape, who is looking to attack your organisation, and what capability they have to do so. Government departments are increasingly looking to strengthen their cyber threat intelligence capabilities as a means of better informing their organisations about the consistently changing and evolving threat landscape, with a view to increase their resilience to cyber-attacks.

The National Cyber Security Strategy 2016-2021 also states that:

*"The administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. New technologies and applications have come to the fore, and greater uptake of internet-based technologies worldwide has offered increasing opportunities for economic and social development. As our reliance on networks in the UK grows, so do the opportunities for those who would seek to compromise our systems and data."*

Government departments are now critically dependant on the internet, however it is becoming better understood how inherently insecure this is. Government departments utilise the internet and externally facing infrastructure to interact with citizens in a vast number of ways such as communicating and making transactions. Different government departments will have varying needs from the internet; therefore, their digital footprints are going to vary greatly.

Threat actors will continuously make attempts to exploit the weaknesses of government departments, and launch attacks to compromise the confidentiality, integrity, and availability of the assets owned and used by departments.

## 1.2 The Problem

As government departments integrate further internet-based technologies and put more information and data online, their digital footprints are becoming increasingly large and complex. A government department will likely have numerous websites, social media accounts, servers, IP ranges, databases, repositories, cloud storage servers and other internet-facing assets. Many departments are likely to have many more assets that the security teams are not aware of, such as ad-hoc sites and services like temporary QA environments which may have been set up by former employees but have since been forgotten. Much of the information within these digital footprints could be of significant value to hostile threat actors. Collectively, these fall under the threats against a government department, within their digital footprint.

If nothing is done to stop this trend, then we can expect government departments to become easier targets to plan and commit attacks against.

## 1.3 The Paper

In researching this problem, we have held 21 engagements across 14 different organisations, including the NCSC, 5 government departments, 3 cross-government functions, 1 university and 5 commercial partners to understand the current capability within the industry, as well as helping to influence the creation of a Capability Maturity Model.

**This paper will provide recommendations as to how government departments can better understand and control their digital footprint through developing and maturing Digital Risk and Intelligence capabilities.**

The recommendations in this paper have been broken down into three levels:

- Threat Intelligence team - the quick, more easily implemented, short term recommendations;
- Government Department - the medium-term recommendations that will bolster the capability of the threat intelligence teams;
- Cross-Government functions - the longer-term recommendations that will allow government departments to better protect their digital footprints for the future.

This has been done to ensure these new capabilities can be implemented, enabled and supported in the most effective way. There are a vast number of organisations, functions and departments in government that can assist in bolstering in-house Digital Risk and Intelligence capabilities.

This report, produced via a literature review and engagements with public and private sector organisations (listed in Appendix I), will outline good practice Digital Risk and Intelligence and provide guidance to government departments to aid the mobilisation and subsequent maturation of their Digital Risk and Intelligence capabilities. The report is structured as follows:

- **Section 2** provides and overview of Digital Risk and Intelligence as a capability and introduces key concepts for the remainder of the report.
- **Section 3 and 4** are targeted at **security managers**, such as heads of SOCs, and outlines the capability required from people, processes and tools for a government department's threat intelligence team or SOC to operate a basic but competent Digital Risk and Intelligence capability and hence reduce risk.
- **Section 5** is targeted at **senior security managers**, such as Chief Information Security Officers (CISOs), and outlines the activities that a government department should take at the enterprise-level to enable the Digital Risk and Intelligence function and hence improve its efficiency and effectiveness.

- **Section 6** is targeted at **decision makers within cross-government functions**, and outlines steps that can be taken by cross-government functions to improve collaboration, set a common baseline, and professionalise the DR&I analyst role and hence improve our collective security.

# 2 What is Digital Risk and Intelligence?

## 2.1 The Cyber Kill Chain

The Cyber Kill Chain (3), originally developed by Lockheed Martin (LM), is an industry-accepted methodology, which provides a step by step guide for tracking and understanding how an attacker will conduct the necessary activities in order to commit a successful attack on an organisation. It details each of the steps in an attack from early reconnaissance stages, through to the successful completion where the intruder achieves their objectives. The LM Cyber Kill Chain assists security teams in detecting and preventing threats, through establishing strong controls and countermeasures, which will serve to protect their organisation's assets. Figure 1 provides a visual representation of the LM Cyber Kill Chain.

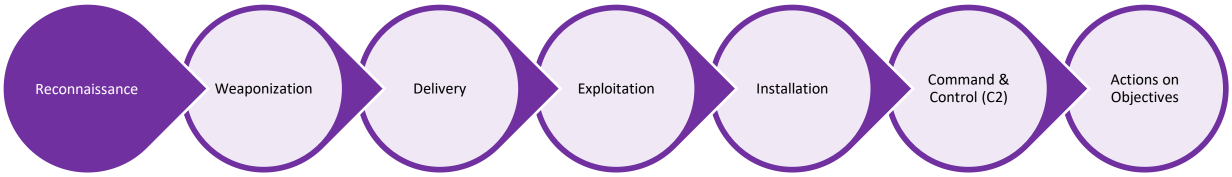


*Figure 1 – The LM Cyber Kill Chain*

During the initial **reconnaissance** stage of the LM Cyber Kill Chain, a threat actor will attempt to gain knowledge about the target organisation, employees and physical locations, including offices and data centres. This is aimed at identifying, and eventually exploiting, key assets and resources which are of value to the organisation and the attacker.

Digital Risk and Intelligence sits fundamentally in the reconnaissance stage of the LM Cyber Kill Chain. The LM Cyber Kill Chain implores security teams to “think like an attacker” which is a crucial element in standing up a Digital Risk and Intelligence capability, as it allows you to target assets that are at most risk (4). Understanding the attacker mindset is a crucial element in reducing the risk of external attacks to the organisation (5).

One example of this would be the fact that many large companies like Facebook Inc. and Microsoft Corp have hired hackers to assist in building their security defences (6). Similarly, some government departments are adopting red teaming activities through initiatives such as GBEST[1].

[1] https://www.gov.uk/government/speeches/speech-by-the-rt-hon-david-lidington-mp-at-london-stock-exchange

## 2.2 Definitions

### 2.2.1 Definition of Digital Risk and Intelligence

"Digital Risk and Intelligence" is not currently a widely used term within the industry, partly due to the fact it has several different names; for example, "Digital Risk Protection" or "Digital Footprint Monitoring". For this paper, we will use the following formal definition of Digital Risk and Intelligence:

**"Digital Risk and Intelligence (DR&I) is the process of monitoring, detecting and remediating threats within the public domain, through the control of an organisation's digital footprint. This is so that issues can be mitigated before threat actors exploit this information, in order to reduce the likelihood of intrusion, and limit the effects of successful attacks when they occur."**

### 2.2.2 Definition of Digital Footprint

A 'digital footprint' is a phrase that is widely used within the industry to describe the trail, traces or "footprints" that people, companies or organisations leave online. Digital footprints can be comprised of all the information manifested online that relates to that person or organisation. These can be hosted on, for example, social media accounts, e-mails and attachments, videos or digital images, web facing infrastructure, online assets, applications (7), and any other form of transmission of information — all of these leave traces of information about individuals or their company, and thus are available to others online.

### 2.2.3 Additional Definitions

For this report, we will also need to define some additional concepts; these cover external sources on which a digital footprint can be found. By 'external sources', we mean the internet and publicly available domains, which can be summarised as the open web, deep web and dark web. The definitions of these terms are given below.

#### 2.2.3.1 Open Web

The "open web" (also known as the "clearnet" or "surface web") is the portion of the internet that is described as being readily available to the general public and searchable through standard web search engines. The open web is made up of web pages that are in a server, available to be accessed, or indexed, by any search engine.[2]

#### 2.2.3.2 Deep Web

The "deep web" (also known as the "invisible web" or "hidden web") are parts of the internet whose contents are described as not being indexed by standard web search engines. Most of the deep web

[2] https://www.pinkhattech.com/2017/12/04/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web/

contains harmless information, but it can also foster serious criminal activity. The deep web is considered as being quite large; several times the size of the surface web.

The content of the deep web is located and accessed by a direct URL or IP address, and is hidden behind HTTP forms. It includes many common uses such as web mail, online banking and services that users must pay for, and pages protected by a paywall, such as video on demand, some online magazines and newspapers, among others.[3]

### 2.2.3.3 Dark Web

The dark web is a portion of the internet for which its content exists on overlay networks that require specific software, configurations, or authorisation to access.[4]

The dark web can be thought of as being comprised of 'dark nets'. These are networks which are small, friend-to-friend/peer-to-peer networks, as well as large, popular networks operated by public organisations and individuals, such as Tor, Freenet, I2P, and Riffle.

The dark web is largely known for illicit trading and somewhere that criminal activity takes place.

Figure 2 provides for a visual representation of a breakdown of the difference between the above definitions.

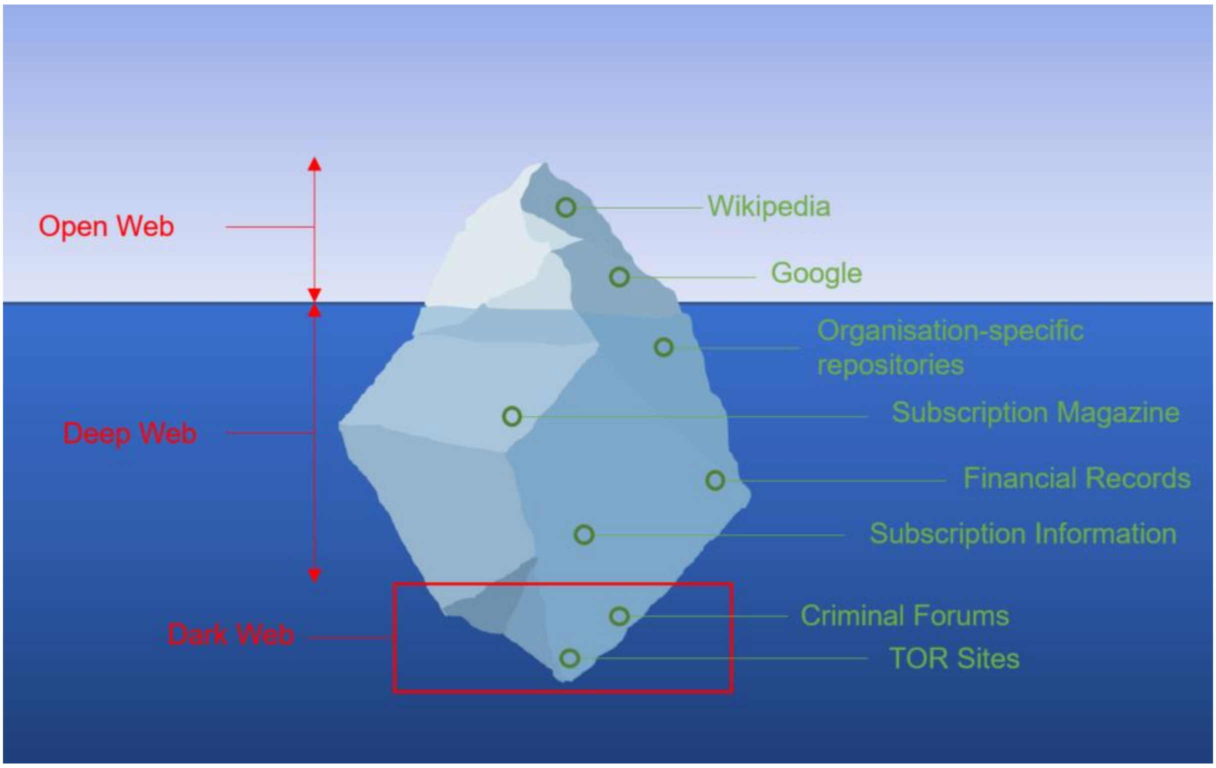


*Figure 2 – External Sources Breakdown*

[3] https://whatis.techtarget.com/definition/deep-Web

[4] https://whatis.techtarget.com/definition/dark-web

## 2.3 Scope

One of the challenges for a government department in assessing their digital footprint is defining the scope of the kinds of activities they want to look for. If we were to search the full breadth of the open, deep and dark web, it would be too broad, inefficient and would take an extremely high level of maturity. For this reason, we have developed seven use cases that create the required scope. This scope will allow threat intelligence teams to have a better understanding of the areas of their digital footprint they should focus on when developing a capability.

The use cases in scope are as follows:

- Information Leakage
- Infrastructure Insight
- Attacker Reconnaissance
- Compromise Research
- Infrastructure Misconfiguration
- Shadow IT
- Employee Footprint

There are also 4 use cases we have identified, as part of our research, that have been removed from our scope:

- VIP Protection
- Third Party Assessment
- Brand and Reputational Damage
- Malicious Mobile Apps

This paper will go through each of these use cases and explain the reasoning for why they are in or out of scope.

## 2.4 Use Cases in Scope

### 2.4.1 Information Leakage

Digital assets that are not intended for public consumption, such as sensitive internal documentation or private email correspondence, can sometimes leak from secure corporate networks into the public domain.

Examples of Information Leakage could include documentation that is protectively marked as OFFICIAL-SENSITIVE but is hosted on an open site or document repository, such as Trello or Huddle. Another example would be employees emailing sensitive documentation from a secure government network to another network that is not appropriately secure.

This information is highly valuable to hostile threat actors and can certainly be utilised against the organisation in a number of ways. Examples include selling of the information for financial gain, making use of the information to commit an attack, or coercing employees to commit insider attacks.

An organisation should be able to identify, or be alerted to, instances when sensitive internal documentation, emails or private correspondence are being hosted on external sources.

*A Digital Risk and Intelligence team should be able to identify, through searching over publicly available domains or being notified, when sensitive internal documentation and private correspondence that is not meant for public consumption is available in the public domain. This is so that the proper action can be taken getting the information removed as quickly as possible.*

### 2.4.2 Infrastructure Insight

One of the biggest concerns for security teams includes trying to mitigate and limit the amount of information online about the IT infrastructure of their organisation. Information about the IT systems is extremely valuable to hostile threat actors in planning attacks against organisations. This kind of information is frequently being uploaded to a number of different public domains, such as:

- Social Media Websites
- Job Advertising Websites
- Technical Forums
- Invitations to Tender

Taking job advertising websites for instance; those posting the vacancy and job role can provide a great deal of information about what the successful applicant will be doing in their roles and in some cases, a concerning amount of information is provided, detailing exactly what systems exist and in what way they are used. This kind of information is incredibly valuable to threat groups, as it can make it much easier for the threat actors to know in what way they should commit successful attacks.

*Digital Risk and Intelligence teams should be able to gain an understanding of what information about their IT infrastructure is available online. This could be through searching the open and deep web services in order to mitigate the sharing of sensitive information.*

### 2.4.3 Attacker Reconnaissance

The reconnaissance stage is the earliest point in the LM Cyber Kill Chain and identifying threat actor reconnaissance activities as soon as possible can mean that security teams can stop an attack long before it has taken place, or at the very least put controls to limit the likelihood of the attack.

Examples of reconnaissance activities could be identifying when possible attackers are conducting port scans of a department's infrastructure or having conversations between threat groups on social media or criminal forums, that detail an upcoming attack on organisations. Examples could also include the creation of misleading domains that resemble that of a government department.

*Digital Risk and Intelligence teams would benefit from being able to detect and identify threat actor reconnaissance activities at the earliest possible opportunity in order to deter an attack taking place and put the necessary controls in place to limit the effects of that attack.*

#### 2.4.3.1 Compromise Research

Another more specific reconnaissance activity is when a large number of login details are pasted, usually through bulk upload, onto a website such as Pastebin, or onto criminal forums on the deep or dark web. In many instances, only a small amount of credentials are posted, with the offer to sell the remainder to another threat actor.

This means that a breach has already taken place, however another breach is very likely to commence and so this needs to be acted on as soon as possible.

If an analyst can successfully identify instances when credentials have been posted or are being sold, then they can mandate the reset of the passwords before the further compromise takes place.

It is also an opportunity for the security teams to understand that a breach has taken place for these credentials to have been leaked, and so can continue to investigate how this has been allowed to happen.

*Digital Risk and Intelligence teams should have the ability to understand or be notified to an instance when employee credentials have been leaked onto publicly available domains, so they can limit the effects at the earliest opportunity.*

### 2.4.4 Shadow IT

Shadow IT is an umbrella term referring to any technology, such as an application or device (smartphone, tablet, laptops, etc.), that is used without following the organisation's governance and approval processes[5]. These systems may not have the necessary security controls in place and in many cases are completely unknown to the security teams. These applications could be used by either individual employees or an entire business unit.

Most employees who adopt unsanctioned solutions do so with good intentions, not to undermine security, but often to increase their effectiveness. With the plethora of business and productivity applications available and the ease of installing these applications, shadow IT continues to propagate. Often, the process of seeking official IT approval for new applications is onerous and long, so employees try to find work arounds for this.

Common shadow IT examples include:

- Productivity apps (Trello, Slack, Asana);
- Cloud storage (Dropbox, Google Drive);

[5] https://en.wikipedia.org/wiki/Shadow_IT

- Communication apps (Skype, VOIP, WhatsApp);
- Externally facing websites, or social media profiles.

Without the appropriate security controls in place, sensitive information about the organisation could easily be leaked to hostile threat actors. There are many wider instances of shadow IT, such as unsanctioned physical devices (flash drives, external drives), but for this context we are concerned with shadow IT that would pose threats to the digital footprint of a government department.

Shadow IT can seriously compromise the security of the organisation. Having sensitive information outside of the control of the security team can have detrimental and devastating effects. If information is being stored outside of the compliant systems, a breach of this information can also have long-lasting effects on the reputation of that organisation.

*Digital Risk and Intelligence teams would benefit from having a better understanding of their organisation's entire public facing infrastructure through searching for and identifying externally facing instances of shadow IT.*

### 2.4.5 Infrastructure Misconfiguration

As government departments are putting more information online, more websites and externally facing assets are being created and added to their infrastructure. There is increasing opportunity for this public facing infrastructure to be misconfigured, and thus more vulnerable to attacks from opportunistic threat actors.

Examples of Infrastructure Misconfiguration can be broken down into two sub use cases:

1. The leaking of information to the public domain through a misconfigured data hosting site, e.g. a misconfigured AWS bucket.
2. Vulnerabilities on external facing portals or websites that would allow access into the organisation's internal infrastructure or databases.

*Digital Risk and Intelligence teams should have the ability to identify and monitor vulnerabilities for their public facing infrastructure, in order to minimise the risk of direct attacks on the infrastructure.*

### 2.4.6 Employee Footprint

What an organisation's employees do and say online can make them and their organisation vulnerable to a range of cyber security threats. Some vulnerabilities can be obvious, such as posting or sharing confidential information that puts employees, processes or assets at risk. Others may be less so, such as search engines storing search history or device tracking geolocation data which may be exploited by those with malicious intent.

Similar to our definition of digital footprint, we can say that an employee's digital footprint is the data that is left behind whenever a person carries out online activities.

Examples of these online activities are as follows:

- Photo sharing;
- Dating;
- Banking;
- Shopping;
- Gaming;
- Professional and social networking.

These can all add to the employee's digital footprint. Other people can also contribute to an individual's digital footprint by posting photographs or information about the individual online. The footprint will therefore be the entirety of the data online about that person, not just the information they put online themselves.

Although many employees will make attempts to separate their personal and professional 'digital lives', all of this information could very easily contribute to the digital footprint of the organisation. Therefore, the digital footprint of the employee could be very valuable to a threat actor, and easily leveraged in an attack.

For example, an employee could unknowingly reveal sensitive information on a publicly available technical special interest forum, and this could give a criminal better guidance on exactly how to attack their organisation. Another example would be an employee displaying their vetting status or clearance on social media, going against the policy of their department.

However, government departments need to be careful not to conduct any level of invasive monitoring of their employees' footprints. Government departments should at no point invade the privacy of its employees. Please see the Employment Practices Code for more information on data protection requirements of employees[6].

*Digital Risk and Intelligence teams would benefit from encouraging employees to better protect and manage their personal and professional digital footprint.*

## 2.5 Use Cases Out of Scope

There are a number of use cases that have been identified through our research, particularly from services offered by vendors. We have put these use cases outside of the scope of the capability; the following section details the reasoning for these decisions.

### 2.5.1 VIP Protection

Employees who are very senior, highly technical, or have very high clearance are sometimes considered "VIPs" and can be specifically targeted by threat actors who are intent on damaging the

[6] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

person's and/or organisation's reputation. Threat actors could also be looking to exploit the person's information and, in some cases their higher privileges, to gain access to internal infrastructure. Access to VIP mailboxes, for example, could reveal both sensitive commercial discussions, as well as allowing convincing spoofing of the VIP and the exploitation of trust relationships between the VIP and other parties.

A service offered by some vendors is the ability to assess the digital footprint of specific individual employees, or VIPs, of a company. They take some of the techniques that this report is applying to a government department but focus it onto a person instead of a whole organisation. In our research engagement with Bank of England, we found that they were doing a large amount of work this area, conducting many instances of VIP Protection, and have found some very useful information. However, the Bank of England is of a much higher maturity than the majority of government departments.

*Why is this not in scope?*

In our research and discussions, we have found that this is something that only organisations with an already very mature Digital Risk and Intelligence capability carry out, or if they have a specific need for it. VIP Protection is too specialist an activity to be appropriately applied to the majority of government departments, and so we have adopted some of the techniques and encompassed them as part of the *Employee Footprint* use case. This use case covers all the needs for providing guidance to employees on how best to control their footprint, but not giving specific guidance to senior individuals.

### 2.5.2 Third Party Assessment

Some Digital Risk and Intelligence vendors offer a service or tool that will allow organisations to carry out assessments of the digital footprint of a possible third-party supplier, e.g. scoring potential supply chain partners using digital evidence. This can be useful for understanding the security of your potential supply chain.

*Why is this not in scope?*

Although this features heavily in vendor offerings, this is something that is usually outsourced to a third party, and that is not what this paper is intended to recommend. This paper recommends that government departments are able to assess their own footprint, as opposed to anyone else's. Assurance of a supply chain is beneficial to government departments, however it is widely considered to be of its own distinct domain in cyber security, and for that reason it is being kept out of scope for the paper.

### 2.5.3 Brand and Reputational Damage

Some organisations adopt a digital footprint mapping capability to manage how their brand is exposed or monitored for potential reputational damage on forums such as social media. This use case is primarily about maintaining the brand of the organisation to uphold trust with the public. This is of great concern for some government departments, for example HMRC have put in substantial effort to bring down the number of spoof HMRC emails and fake domains, in order to maintain trust with citizens.

*Why is this not in scope?*

Although this is a legitimate concern for the reputation of the department, we are more focused on the cyber security aspect of digital footprint mapping, and not on brand awareness or brand management. Therefore, we have kept this out of scope. With regards to this paper, the cyber security aspect of Digital Risk and Intelligence is of much more concern than the need for specific brand awareness.

### 2.5.4 Malicious Mobile Apps

One type of threat that is closely related to Digital Risk and Intelligence is the creation of malicious apps that have been created by threat groups in order to impersonate government apps, usually used for phishing purposes.

*Why is this not in scope?*

Although this is a growing area of Digital Risk and Intelligence, we have considered this out of scope to ensure that threat intelligence teams can set up the basics of a capability before tackling wider issues such as this. We believe that this is something that can only be done by organisations that already have a mature Digital Risk and Intelligence capability.

Ideally, we would want organisations to be able to tackle this issue, however from our research into this area, and validating our scope with industry partners and vendors, the message has been to work through the use cases identified in our scope before entering into higher levels of maturity.

Figure 3 below provides an understanding of the connections between the in-scope and out of scope use cases.

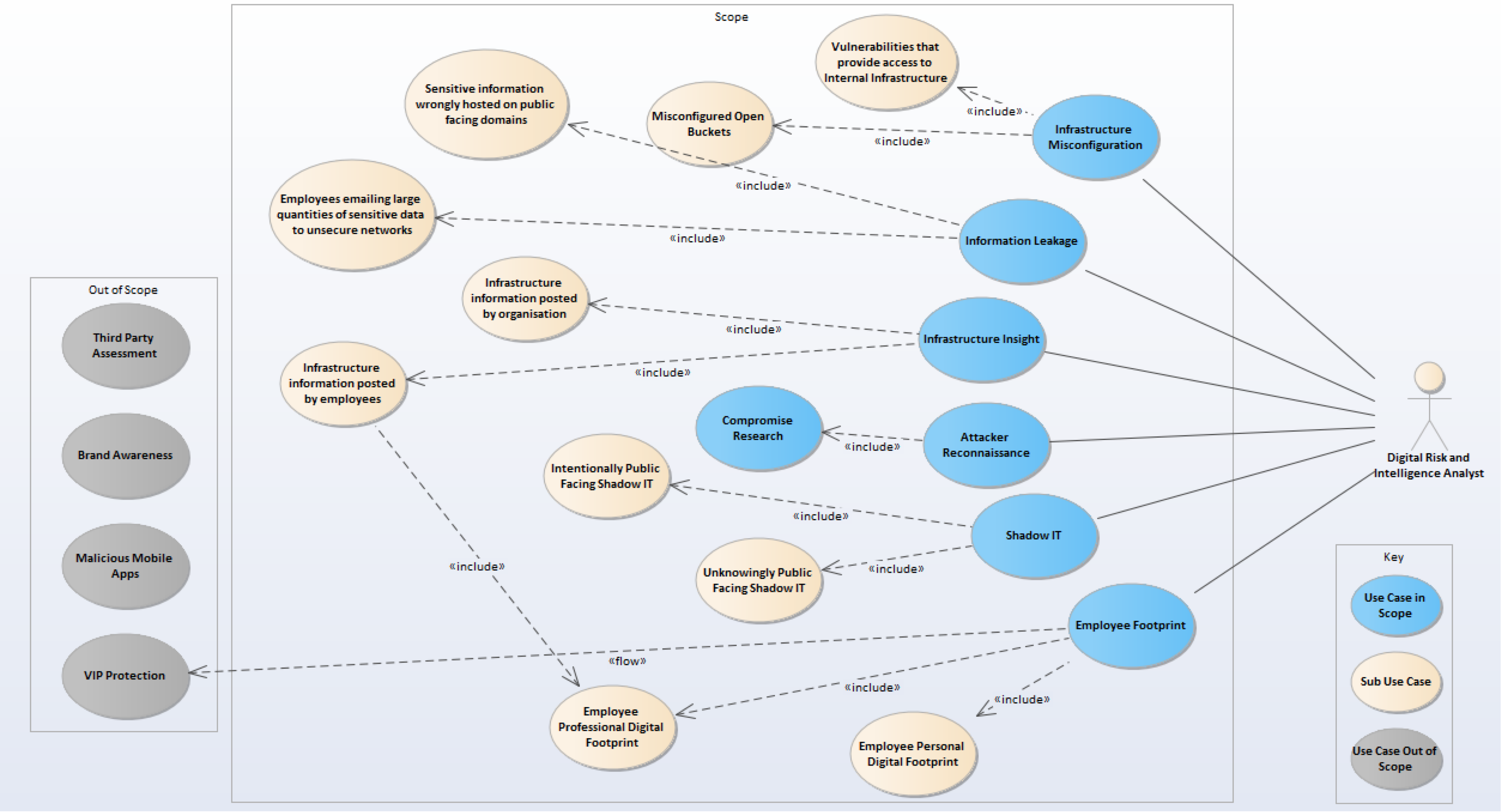

Scope
Vulnerabilities that provide access to Internal Infrastructure
Sensitive information wrongly hosted on public facing domains
Misconfigured Open Buckets
«include»
«include»
Infrastructure Misconfiguration
«include»
Employees emailing large quantities of sensitive data to unsecure networks
«include»
Information Leakage
Infrastructure information posted by organisation
«include»
Infrastructure Insight
Infrastructure information posted by employees
«include»
Compromise Research
Attacker Reconnaissance
«include»
Intentionally Public Facing Shadow IT
«include»
Shadow IT
Unknowingly Public Facing Shadow IT
«include»
«include»
Employee Footprint
«flow»
«include»
«include»
Employee Professional Digital Footprint
Employee Personal Digital Footprint
Digital Risk and Intelligence Analyst
Out of Scope
Third Party Assessment
Brand Awareness
Malicious Mobile Apps
VIP Protection
Key
Use Case in Scope
Sub Use Case
Use Case Out of Scope

*Figure 3 – Use Case Diagram*

# 3 Building a Digital Risk and Intelligence Roadmap

## 3.1 Overview

A Digital Risk and Intelligence capability should be wrapped up within an existing cyber security capability. The new DR&I team should sit within either the Threat Intelligence team of the government department, or the department's CSOC (Cyber Security Operations Centre).

Some form of self-assessment needs to take place before a government department can take the necessary steps to develop and mature a Digital Risk and Intelligence capability. Each government department has a different risk appetite, and different ways of interacting with the public domain. This needs to be considered alongside the self-assessment to make a strong foundation for maturing their capability.

In this section we will go through how to identify and prioritise your digital assets and points of exposure, and how to self-assess your current capability using the Capability Maturity Model.

## 3.2 Do I Need Digital Risk and Intelligence?

Departments are not (currently) mandated to collect, integrate or analyse threats to their digital footprint, or any form of Cyber Threat Intelligence (CTI). The NCSC minimum cyber security standard presents a minimum set of measures (8), including:

> "As a minimum, Departments shall capture events that **could** be combined with common threat intelligence sources e.g. Cyber Security Information Sharing Partnership (CiSP) to detect known threats."

This states that departments shall collect data (from their own infrastructure and devices) but that integration with CTI, and by extension DR&I, is not mandatory. However, the standard also says that departments should look to exceed the standard wherever possible, so whilst it is not currently mandated that organisations consume threat intelligence content, it is recommended that they do so.

Irrespective of the minimum standard, Digital Risk and Intelligence is likely to be valuable to departments who already have a mature cyber security posture. Whilst the appropriate pre-requisites for a capability to deliver value will vary from department to department, we would recommend as a catch-all statement that organisations only consider significant investment into DR&I after they have met or are on a realistic roadmap to achieving *all* of the 10 sections of the minimum cyber security standard.

## 3.3 Understanding the Elements of a Digital Footprint

The first step towards understanding the organisation's digital footprint includes creating a list of what assets or information is most at risk, and what points of the open web, deep web and dark web are of most concern.

In this section we will detail how and why government departments should list:

- the **digital assets** that are most valued, as well as the most at risk; and
- the **points of exposure** that are of most threat to the department's digital footprint.

### 3.3.1 Taxonomy of Digital Assets

In order for an organisation to better understand their digital footprint, they need to define an appropriate taxonomy of digital assets that are mostly likely to be at risk. We can define a digital asset as:

> *Any piece of property, that can be found in digital form and comes with the right to use, which would be identified as an element of the organisation's digital footprint.*[7]

Government departments will have a whole host of different digital assets which could be found in the public domain. Creating this taxonomy will allow government departments to understand what they should be searching for in the public domain. This taxonomy can also be created through reusing or extending an already existing information asset register.

Examples of these digital assets include:

- Domains
- IP Addresses
- Social Media Accounts
- Server Names
- Sensitive Keywords
- Technical Information Within Email Headers and Footers
- Staff Members' Personal Information
- Organisational Information, Department or Project Names
- Document Titles
- Intellectual Property
- Names of Suppliers
- Protective Marking Scheme
- Code Identifiers
- Code Formats

[7] https://www.computerweekly.com/blog/CW-Developer-Network/What-is-a-digital-asset

- Database Table Names

Government departments should develop an understanding of the impact of compromise for each of the assets. This will also help the team shape and prioritise their scope of operations (as in Section 4). Similarly, this will allow the commissioning of digital footprint maps by third party specialists to be tailored to the needs of the government department, by highlighting the areas of concern.

### 3.3.2 Points of Exposure

For a government department to understand where on the open web, deep web and dark web they should be searching and monitoring for digital assets, they should define a list of points of exposure.

If the taxonomy of digital assets is “what to look for”, then we can say the points of exposure are “where to look”. We can define the points of exposure as:

> *All areas where digital assets, or elements of an organisation’s digital footprint, can be found.*

Government departments would benefit from prioritising which points of exposure are of most threat to them.

One example would be Search Engines. These can generally search over the open web, and therefore identify instances of a government department’s digital footprint – i.e. instances of sensitive documentation that has been leaked (i.e. **Information Leakage**), or displaying elements of **Shadow IT**.

Social Media Websites, such as LinkedIn, Twitter and Facebook can of course host instances of **Employee Footprint**, but as well as this, threat groups could easily have discussions around reconnaissance activities and planned upcoming attacks on government departments (**Attacker Reconnaissance**).

Paste Sites such as Pastebin, can host sensitive information or even documentation (**Information Leakage**), can host instances of **Compromise Research**.

File Sharing websites can host and share documents and large files, which allows threat actors to send and receive stolen sensitive documentation (**Information Leakage**), and large bulk files of login details (**Compromise Research**).

Cloud storage services, such as AWS buckets, that have been set up by a government department can sometimes be misconfigured (**Infrastructure Misconfiguration**) and therefore could be open or leaking sensitive information (**Information Leakage**).

Dark web Criminal Forums and Markets are other examples of point of exposures, as this is where threat actors could be discussing reconnaissance activities (**Attacker Reconnaissance**), as well as buying/selling sensitive information about government departments or login details (**Information Leakage**, **Compromise Research**).

Infrastructure Search Engines, e.g. Shodan or Censys, can display large amount of information of a government departments infrastructure (**Infrastructure Insight**), and can also be used to identify instances of **Shadow IT**.

Job Advertising websites, when advertising upcoming roles, particularly in technology, can sometimes display detailed information of about the IT estate in the government department (**Infrastructure Insight**), which can allow threat actors to have a better understanding of how to commit an attack against the department.

Another very prominent point of exposure for government departments is that of Code Repositories, namely GitHub. In our engagements research, such as discussions with the Government Digital Service, they identified instances of large amounts of open source code detailing the specifics of their infrastructure. This is available for threat actors to view, steal, manipulate and give them a better understanding on how to attack the department's systems (**Infrastructure Insight**). As well as that, GitHub also provides the names, and sometimes photos of the individuals working on that code, which would be very valuable to threat actors. On occasion, GitHub repositories have been known to include passwords that have been hardcoded into the source code of a project, available to view by the public.

Here is a list possible points of exposure, from which DR&I teams can start from:

- Search Engines
- Social Media
- Infrastructure Search Engines – e.g. Shodan
- Whois and DNS Information
- Paste Sites – e.g. Pastebin
- File Sharing Sites
- Cloud Storage Services
- Code Repositories – e.g. Github
- Technical Forums
- FTP Servers
- Threat Actor Blogs
- I2P and ToR
- Messaging Platforms
- Dark web Criminal Forums and Markets
- Job Advertising Sites
- Invitations to Tender

## 3.4 Capability Maturity Model

The following Digital Risk and Intelligence Capability Maturity Model (CMM), shown in Table 1, comprises five levels of maturity from Level 1 (Initial) to Level 5 (Optimising). These are broken down into the sub-capabilities of People, Process and Tools.

The Capability Maturity Model has been developed through extensive research, and numerous engagements with government departments and commercial partners, all with Digital Risk and Intelligence Capabilities of varying levels of maturity. This research has allowed us to create a model for which government departments can use to make critical decisions about how they can realistically mature their capability.

As part of the research for the paper, we have identified mixed impressions of maturity models, and this is something we have taken on board when producing this section of the paper. We advise that you do not use the model as a yardstick, but instead use it to re-enforce continual improvement of capabilities in your cyber security function. The maturity model is only useful if it is used appropriately to improve the DR&I capability in your organisation[8]. This needs to be kept in mind when using the maturity model.

### 3.4.1 Level 1 – Initial

Level 1 describes an organisation that performs little or no Digital Risk and Intelligence, and instead takes a reactive stance, either responding to alerts from organisations like the NCSC, or not receiving any alerts at all regarding their digital footprint.

Any digital footprint monitoring that does occur is ad-hoc and basic, performed by generalist staff, such as members of the SOC or threat intelligence team, and often on their own initiative. These organisations will have a narrow understanding of what areas of the digital footprint is of most risk, and what digital assets are currently exposed. Little exists in terms of recruitment or training plans, performance management, or career development. No defined job role with regards to Digital Risk and Intelligence exists.

### 3.4.2 Level 2 – Managed

At Level 2, effort has been taken to start implementing a proactive Digital Risk and Intelligence capability. A responsible resource will utilise a number of basic open source tools to conduct ad-hoc searching with basic alerts set up, such as Google Alerts. There will be some undefined scraping across open web sources.

Recruitment, training, performance and career development are all informally managed. The team is searching over an undefined list of digital assets and assessing only a small portion of the

[8] https://www.ncsc.gov.uk/blog-post/maturity-models-cyber-security-whats-happening-iamm

necessary points of exposure, such as social media and the open web, whilst the legal obligations may not be fully considered.

### 3.4.3 Level 3 – Defined

Level 3 should be the aspired level of maturity for any government department that does not yet operate a Digital Risk and Intelligence capability.

A dedicated team of possibly one resource works against a team charter and follows a formalised and clearly defined scope of operations to assess their defined points of exposure on a regular schedule. Plans for recruitment (if necessary), training and career development are all formally documented, with performance expectations defined.

The team have clear understanding of the business context of their scope. An assessment from a third-party supplier of the entire digital footprint advises the team on what areas are particularly vulnerable, and how they should adjust their scope accordingly. This is done every six months on average.

Shadow IT is actively minimised through being identified in public domains, and appropriately addressed.

### 3.4.4 Level 4 – Quantitatively Managed

At Level 4, the Digital Risk and Intelligence capability is well established, and utilises quantitative metrics to improve performance and display benefit.

The team is supplemented by generalist staff on a rotational basis, both to increase the resources available, but also to develop and motivate the wider SOC staff.

At this level, succession plans are in place for key roles, and performance is tracked at a team level using metrics. Response plans to DR&I incidents are well integrated into the overall threat intelligence response plans. The team regularly review the mean-time-to-remediate (MTTR) of incidents, to assess the performance of the capability. An overall assessment of the digital footprint is done by a third-party supplier on a quarterly basis. The team has good coverage across a variety of sources on the open web, deep web and dark web.

Specific threat intelligence feeds relevant to Digital Risk and Intelligence are received. The team utilises strong relationships with other relevant areas in the business, to understand developing threats in the public domain. External searches of instances for shadow IT are done regularly to try and minimises the risk.

### 3.4.5 Level 5 – Optimising

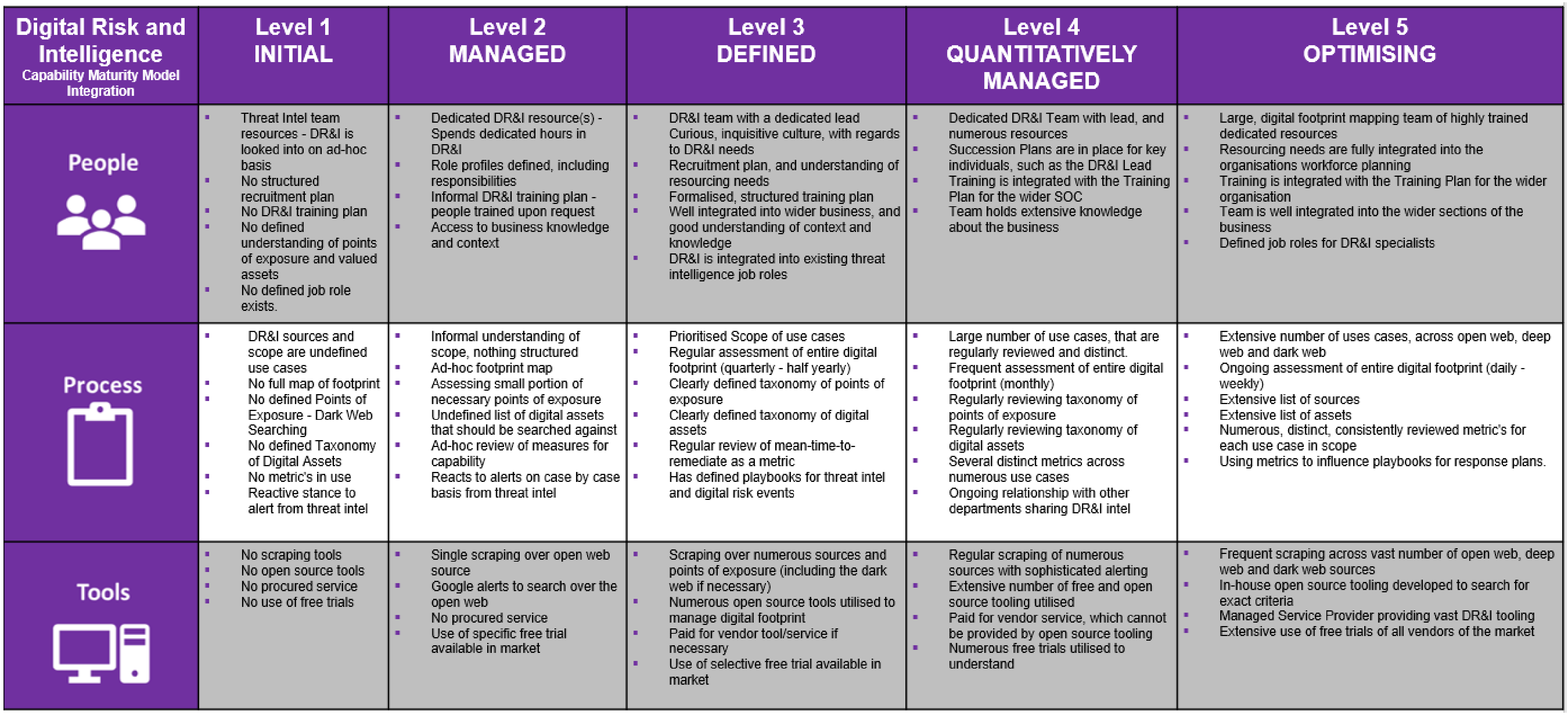
Level 5 represents an advanced Digital Risk and Intelligence capability that should be aspired to, but for many organisations may be unrealistic to achieve.

At this level, the team is fully integrated into the wider SOC and organisation in terms of resourcing, recruitment, training and performance, with action plans created to mitigate any underperformance.

Analysts are well experienced and possess highly developed business knowledge, to understand the changing threats to all externally facing areas of the department. The scope is highly-developed and defined, with a hugely encompassing number of uses cases. Numerous metrics are used to measure the performance of the capability.

A well-integrated procured tool scrapes for information of interest, with well-defined criteria, across all major external sources, in the open web, deep web and dark web. Automated alerts are received and assessed by analysts.

A blend of highly developed in-house tooling, and third-party tools provide an ongoing assessment of the entire digital footprint, as well as searches for instances of shadow IT, takes place on a more than weekly basis.



| Digital Risk and Intelligence<br>Capability Maturity Model Integration | Level 1<br>INITIAL | Level 2<br>MANAGED | Level 3<br>DEFINED | Level 4<br>QUANTITATIVELY MANAGED | Level 5<br>OPTIMISING |
|---|---|---|---|---|---|
| People | ▪ Threat Intel team resources - DR&I is looked into on ad-hoc basis<br>▪ No structured recruitment plan<br>▪ No DR&I training plan<br>▪ No defined understanding of points of exposure and valued assets<br>▪ No defined job role exists. | ▪ Dedicated DR&I resource(s) - Spends dedicated hours in DR&I<br>▪ Role profiles defined, including responsibilities<br>▪ Informal DR&I training plan - people trained upon request<br>▪ Access to business knowledge and context | ▪ DR&I team with a dedicated lead Curious, inquisitive culture, with regards to DR&I needs<br>▪ Recruitment plan, and understanding of resourcing needs<br>▪ Formalised, structured training plan<br>▪ Well integrated into wider business, and good understanding of context and knowledge<br>▪ DR&I is integrated into existing threat intelligence job roles | ▪ Dedicated DR&I Team with lead, and numerous resources<br>▪ Succession Plans are in place for key individuals, such as the DR&I Lead<br>▪ Training is integrated with the Training Plan for the wider SOC<br>▪ Team holds extensive knowledge about the business | ▪ Large, digital footprint mapping team of highly trained dedicated resources<br>▪ Resourcing needs are fully integrated into the organisations workforce planning<br>▪ Training is integrated with the Training Plan for the wider organisation<br>▪ Team is well integrated into the wider sections of the business<br>▪ Defined job roles for DR&I specialists |
| Process | ▪ DR&I sources and scope are undefined use cases<br>▪ No full map of footprint<br>▪ No defined Points of Exposure - Dark Web Searching<br>▪ No defined Taxonomy of Digital Assets<br>▪ No metric's in use<br>▪ Reactive stance to alert from threat intel | ▪ Informal understanding of scope, nothing structured<br>▪ Ad-hoc footprint map<br>▪ Assessing small portion of necessary points of exposure<br>▪ Undefined list of digital assets that should be searched against<br>▪ Ad-hoc review of measures for capability<br>▪ Reacts to alerts on case by case basis from threat intel | ▪ Prioritised Scope of use cases<br>▪ Regular assessment of entire digital footprint (quarterly - half yearly)<br>▪ Clearly defined taxonomy of points of exposure<br>▪ Clearly defined taxonomy of digital assets<br>▪ Regular review of mean-time-to-remediate as a metric<br>▪ Has defined playbooks for threat intel and digital risk events | ▪ Large number of use cases, that are regularly reviewed and distinct.<br>▪ Frequent assessment of entire digital footprint (monthly)<br>▪ Regularly reviewing taxonomy of points of exposure<br>▪ Regularly reviewing taxonomy of digital assets<br>▪ Several distinct metrics across numerous use cases<br>▪ Ongoing relationship with other departments sharing DR&I intel | ▪ Extensive number of uses cases, across open web, deep web and dark web<br>▪ Ongoing assessment of entire digital footprint (daily - weekly)<br>▪ Extensive list of sources<br>▪ Extensive list of assets<br>▪ Numerous, distinct, consistently reviewed metric's for each use case in scope<br>▪ Using metrics to influence playbooks for response plans. |
| Tools | ▪ No scraping tools<br>▪ No open source tools<br>▪ No procured service<br>▪ No use of free trials | ▪ Single scraping over open web source<br>▪ Google alerts to search over the open web<br>▪ No procured service<br>▪ Use of specific free trial available in market | ▪ Scraping over numerous sources and points of exposure (including the dark web if necessary)<br>▪ Numerous open source tools utilised to manage digital footprint<br>▪ Paid for vendor tool/service if necessary<br>▪ Use of selective free trial available in market | ▪ Regular scraping of numerous sources with sophisticated alerting<br>▪ Extensive number of free and open source tooling utilised<br>▪ Paid for vendor service, which cannot be provided by open source tooling<br>▪ Numerous free trials utilised to understand | ▪ Frequent scraping across vast number of open web, deep web and dark web sources<br>▪ In-house open source tooling developed to search for exact criteria<br>▪ Managed Service Provider providing vast DR&I tooling<br>▪ Extensive use of free trials of all vendors of the market |

*Table 1 – Capability Maturity Model*

## 3.5 Assessing Your Current Capability

Government departments need to conduct an assessment to identify what level their capability is currently at, and also what level of maturity they wish to achieve. This map will assist a government department in creating a roadmap for what improvements need to be made to the people, processes and tools of a Digital Risk and Intelligence capability to achieve the desired level of maturity.

**RECOMMENDATION 1: This paper recommends that threat intelligence teams assess their current Digital Risk and Intelligence capability against the provided Capability Maturity Model and then assess the maturity level they wish to realistically achieve.**

# 4 Implementing a Digital Risk and Intelligence Capability

## 4.1 Overview

This section will go through the recommendations for the first of the three levels: the **threat intelligence teams**. For most government departments, Digital Risk and Intelligence teams will sit within existing threat intelligence teams.

These recommendations should allow a government department to build and develop a Digital Risk and Intelligence capability as part of their existing teams. This section of the paper will provide recommendations to do the following:

- Appoint a DR&I team lead, most likely from the cyber threat intelligence team, who can dedicate time to DR&I activities
- Define the scope of the DR&I capability, and a team charter, to ensure the appropriate areas of the footprint will be focused on
- Adopt a series of low cost, publicly available tools as Quick Wins, to easily manage the digital footprint of a government department
- Engage with senior business leaders and internal security teams to build an understanding of the necessary business context and knowledge for the capability to prioritise important areas of the digital footprint, to determine which use cases are of most value
- Integrate DR&I as part of the response plans already established, so that teams can appropriately prepare for and tackle incidents as they occur

These recommendations can also be considered the short-term, more easily achievable options for building and implementing the capability.

## 4.2 Resourcing a Digital Risk and Intelligence Team

From our research engagements with government departments, it was clear that Digital Risk and Intelligence capabilities would sit within existing Threat Intelligence teams. If no Digital Risk and Intelligence capability currently exists, then we recommend Threat Intelligence teams define a Digital Risk and Intelligence team to make a successful start on building a capability. This means allocating a specific number of resources that would act as the Digital Risk and Intelligence team.

There may be some cases in which it would be more appropriate for a new DR&I capability to sit within another team of the department, such a Governance, Risk & Assurance team. If this is the case, then that would still be suitable, however the DR&I team would still need to be in regular contact with the department’s CSOC or Threat Intelligence team.

The first step in resourcing a Digital Risk and Intelligence team and maturing the capability, should be the recruitment or training of a dedicated Digital Risk and Intelligence lead. This lead role is essential in providing direction and technical expertise to more generalist staff that will allow them to start monitoring the public domain in a structured manner. This team lead can be defined as being responsible for the DR&I activities that will be undertaken by the team.

This “team” could be just the capability lead who devotes specific time to Digital Risk and Intelligence activities for **at least half a day a week**. Once the team has been established, the Digital Risk and Intelligence capability can begin its maturation.

**RECOMMENDATION 2: This paper recommends that threat intelligence teams resource a Digital Risk and Intelligence team, starting with assigning a resource as the team lead.**

## 4.3 Identifying Scope of Operations

One of the challenges an organisation can face in developing this capability is assessing the scope of what areas of the digital footprint they should focus on. A Digital Risk and Intelligence team cannot realistically cover the entirety of the open web, the deep web and dark web for every possible threat to their organisation.

For that reason, we recommend that those developing or maturing a new capability identify a **Scope of Operations** that is most relevant to their needs as a department. Something that has been very clear from the research undertaken for this paper is that different government departments will have different priorities regarding their digital footprint, and which areas and external sources they need to focus on. Differences between these government departments could be that they are more policy led, or they could be more transactional, or even citizen vs sector focussed. The way in which a government department interacts with the public domain will ultimately affect which of the digital assets and points of exposure are of most importance to the Digital Risk and Intelligence teams.

A newly-formed Digital Risk and Intelligence capability should take the use cases identified in Section 2.4, and appropriately decide on which use cases are of most concern to the information in their organisation. This needs to be aligned with the risk appetite of that department to ensure that the suitable risk-based approach is taken.

This will help the team develop a tailored capability to tackle the biggest problems facing their digital footprint at the earliest stage – and to make the most of the resources and tooling available. A well-defined scope will allow Digital Risk & Intelligence teams to successfully focus their efforts in the correct areas, given that they are appropriately informed by the business context of the organisation.

**RECOMMENDATION 3: This paper recommends that Digital Risk and Intelligence teams should identify and define a prioritised scope of operations for which areas of the department’s digital footprint they should focus on.**

### 4.3.1 MITRE PRE-ATT&CK Framework

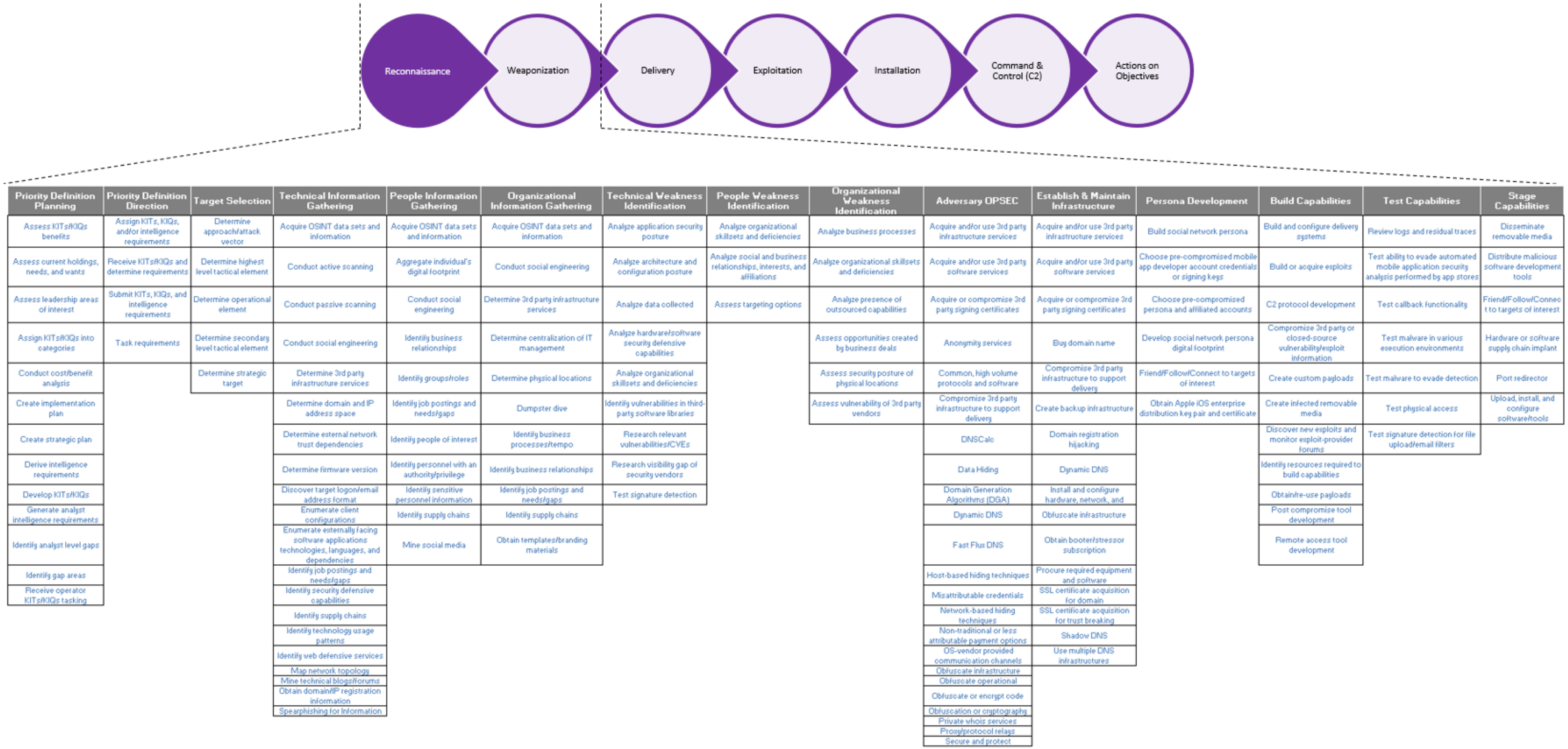
The MITRE PRE-ATT&CK Framework provides the ability to prevent an attack before the threat actor has a chance to get in. The framework comprises of 15 tactic categories, which have been derived from the first two stages of the LM Cyber Kill Chain. It captures the tactics, techniques, and procedures adversaries use to select a target, obtain information, and launch a campaign of attack against an organization. This framework will assist analysts in taking the approach of “thinking like an attacker”.

The framework lists the ways that adversaries perform each tactic and provides the ability to track and organize adversary statistics and patterns. Ultimately, the framework arms defenders with a broader understanding of adversary actions that they can use to determine technical or policy-based mitigations and evaluate the areas of weakness of their digital footprint.

The framework includes tactics and techniques across both the Reconnaissance and Weaponization phases of the LM Cyber Kill Chain, so analysts should keep that in mind when assessing which of the tactics and techniques they wish to utilize.

**RECOMMENDATION 4: This paper recommends that Digital Risk and Intelligence teams adopt the MITRE PRE-ATTA&CK Framework in order assist in defining what areas of their digital footprint they should be focussing on.**

Figure 7 displays the MITRE PRE-ATT&CK Matrix, and the corresponding areas of the LM Cyber Kill Chain.



| Priority Definition Planning | Priority Definition Direction | Target Selection | Technical Information Gathering | People Information Gathering | Organizational Information Gathering | Technical Weakness Identification | People Weakness Identification | Organizational Weakness Identification | Adversary OPSEC | Establish & Maintain Infrastructure | Persona Development | Build Capabilities | Test Capabilities | Stage Capabilities |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Assess KITs/KIQs benefits | Assign KITs, KIQs, and/or intelligence requirements | Determine approach/attack vector | Acquire OSINT data sets and information | Acquire OSINT data sets and information | Acquire OSINT data sets and information | Analyze application security posture | Analyze organizational skillsets and deficiencies | Analyze business processes | Acquire and/or use 3rd party infrastructure services | Acquire and/or use 3rd party infrastructure services | Build social network persona | Build and configure delivery systems | Review logs and residual traces | Disseminate removable media |
| Assess current holdings, needs, and wants | Receive KITs/KIQs and determine requirements | Determine highest level tactical element | Conduct active scanning | Aggregate individual's digital footprint | Conduct social engineering | Analyze architecture and configuration posture | Analyze social and business relationships, interests, and affiliations | Analyze organizational skillsets and deficiencies | Acquire and/or use 3rd party software services | Acquire and/or use 3rd party software services | Choose pre-compromised mobile app developer account credentials or signing keys | Build or acquire exploits | Test ability to evade automated mobile application security analysis performed by app stores | Distribute malicious software development tools |
| Assess leadership areas of interest | Submit KITs, KIQs, and intelligence requirements | Determine operational element | Conduct passive scanning | Conduct social engineering | Determine 3rd party infrastructure services | Analyze data collected | Assess targeting options | Analyze presence of outsourced capabilities | Acquire or compromise 3rd party signing certificates | Acquire or compromise 3rd party signing certificates | Choose pre-compromised persona and affiliated accounts | C2 protocol development | Test callback functionality | Friend/Follow/Connect to targets of interest |
| Assign KITs/KIQs into categories | Task requirements | Determine secondary level tactical element | Conduct social engineering | Identify business relationships | Determine centralization of IT management | Analyze hardware/software security defensive capabilities | | Assess opportunities created by business deals | Anonymity services | Buy domain name | Develop social network persona digital footprint | Compromise 3rd party or closed-source vulnerability/exploit information | Test malware in various execution environments | Hardware or software supply chain implant |
| Conduct cost/benefit analysis | | Determine strategic target | Determine 3rd party infrastructure services | Identify groups/roles | Determine physical locations | Analyze organizational skillsets and deficiencies | | Assess security posture of physical locations | Common, high volume protocols and software | Compromise 3rd party infrastructure to support delivery | Friend/Follow/Connect to targets of interest | Create custom payloads | Test malware to evade detection | Port redirector |
| Create implementation plan | | | Determine domain and IP address space | Identify job postings and needs/gaps | Dumpster dive | Identify vulnerabilities in third-party software libraries | | Assess vulnerability of 3rd party vendors | Compromise 3rd party infrastructure to support delivery | Create backup infrastructure | Obtain Apple iOS enterprise distribution key pair and certificate | Create infected removable media | Test physical access | Upload, install, and configure software/tools |
| Create strategic plan | | | Determine external network trust dependencies | Identify people of interest | Identify business processes/tempo | Research relevant vulnerabilities/CVEs | | | DNSCalc | Domain registration hijacking | | Discover new exploits and monitor exploit-provider forums | Test signature detection for file upload/email filters | |
| Derive intelligence requirements | | | Determine firmware version | Identify personnel with an authority/privilege | Identify business relationships | Research visibility gap of security vendors | | | Data Hiding | Dynamic DNS | | Identify resources required to build capabilities | | |
| Develop KITs/KIQs | | | Discover target logon/email address format | Identify sensitive personnel information | Identify job postings and needs/gaps | Test signature detection | | | Domain Generation Algorithms (DGA) | Install and configure hardware, network, and | | Obtain/re-use payloads | | |
| Generate analyst intelligence requirements | | | Enumerate client configurations | Identify supply chains | Identify supply chains | | | | Dynamic DNS | Obfuscate infrastructure | | Post compromise tool development | | |
| Identify analyst level gaps | | | Enumerate externally facing software applications technologies, languages, and dependencies | Mine social media | Obtain templates/branding materials | | | | Fast Flux DNS | Obtain booter/stressor subscription | | Remote access tool development | | |
| Identify gap areas | | | Identify job postings and needs/gaps | | | | | | Host-based hiding techniques | Procure required equipment and software | | | | |
| Receive operator KITs/KIQs tasking | | | Identify security defensive capabilities | | | | | | Misattributable credentials | SSL certificate acquisition for domain | | | | |
| | | | Identify supply chains | | | | | | Network-based hiding techniques | SSL certificate acquisition for trust breaking | | | | |
| | | | Identify technology usage patterns | | | | | | Non-traditional or less attributable payment options | Shadow DNS | | | | |
| | | | Identify web defensive services | | | | | | OS-vendor provided communication channels | Use multiple DNS infrastructures | | | | |
| | | | Map network topology | | | | | | Obfuscate infrastructure | | | | | |
| | | | Mine technical blogs/forums | | | | | | Obfuscate operational | | | | | |
| | | | Obtain domain/IP registration information | | | | | | Obfuscate or encrypt code | | | | | |
| | | | Spearphishing for Information | | | | | | Obfuscation or cryptography | | | | | |
| | | | | | | | | | Private whois services | | | | | |
| | | | | | | | | | Proxy/protocol relays | | | | | |
| | | | | | | | | | Secure and protect | | | | | |

*Figure 4 - MITRE PRE-ATT&CK Matrix and the LM Cyber Kill Chain*

### 4.3.2 Team Charter

Following on from the scope of operations, a team charter should be established to clarify the direction and approach the team should be taking, whilst setting up the clear boundaries for what the team are searching for and, importantly, what they are not searching for. This will illustrate the direction of the team and will reduce any confusion around objectives and use cases further down the line.

The team charter should also articulate the role of the analysts and the value of Digital Risk and Intelligence as a capability, so this can be traced back from when analysts are carrying out their activities.

**RECOMMENDATION 5: This paper recommends that Digital Risk and Intelligence teams should create a team charter in order to appropriately define the boundaries for what the analysts will be searching publicly available domains for.**

## 4.4 Business Knowledge and Context

We recommend that Digital Risk and Intelligence teams hold, utilise and apply the necessary business context and knowledge in order to ensure the correct approach is taken in creating and developing the capability.

With the correct and relevant business knowledge, the team will be able to successfully focus their efforts into the areas of their digital footprint that matter the most to their organisation and can thus apply the correct security management processes. As previously stated, different government departments will have different prioritised needs from a capability. How a government department interacts with citizens using external infrastructure will ultimately change how their digital footprint is going to look, and therefore will affect what kind of threats there will be against them. For example, if a government department interacts with and receives payments from citizens, then the threats to their digital footprint will vary considerably compared with a department who interacts more with county councils than citizens.

Some level of engagement with senior business leaders should take place. These individuals should be able to provide a breakdown of the ownership of the digital assets and can therefore assist in setting priorities about how to approach the mapping of the digital footprint.

The Digital Risk and Intelligence team will need to build strong relationships with the internal security teams within the department, for example Personnel Security and Information Security teams. The new capability will need to be in alignment with the policies of these teams, such as specific policies relating to privacy or HR.

Having these strong relationships will also optimise the way in which DR&I incidents are handed off to the necessary recipient to remediate. If these teams work together, the DR&I team will hold a better understanding of the best way to hand off incidents relating to Employee Footprint for the Personnel Security team, and incidents of Information Leakage for the Information Security teams.

The correct incident response plans will then be established, and incidents can be remediated quicker and more effectively.

Digital Risk and Intelligence teams would also benefit from receiving the outputs of vulnerability scans and penetration test results, which would inform their scope with regards to Infrastructure Misconfiguration.

Digital Risk and Intelligence teams who hold a good understanding of the business context can then effectively prioritise their scope of operations that they will be focussing on.

**RECOMMENDATION 6: This paper recommends that Digital Risk and Intelligence teams engage with senior business leaders in their department, including internal security teams, in order to provide an understanding of the necessary business context and knowledge for the capability to successfully monitor and control their digital footprint.**

## 4.5 Quick Wins and Open Source Tooling

There is a large number of Free and Open Source Software (FOSS) currently available that will assist government departments in identifying threats in their digital footprint. We have given a short summary of easily useable tools to get an organisation with little or no Digital Risk and Intelligence capability to do some degree of digital footprint monitoring.

These tools and services can be considered as candidate “Quick Win” solutions that threat intelligence teams can implement and utilise in order to rapidly create some form of capability to build upon.

These include setting up breach notifications, hostile reconnaissance and scraping open source intel.

The following page displays the candidate Quick Wins. These have been colour coded in terms of difficulty of their implementation. Those highlighted in green are easier to do, whereas those on which are red and black are harder to carry out. This can allow teams with very low maturity to know where to start when creating a capability, and to make the most of the open source tooling that is available.

The Quick Wins are broken down into three sections:

- Alerting and Automated Tools
- Communities
- Searching and Scraping Tools

**RECOMMENDATION 7: This paper recommends that Digital Risk and Intelligence teams exploit the candidate Quick Wins to create a significant level of capability to monitor and control the digital footprint of the government department.**

## Alerting and Automated Tools

| Google Alerts | Have I Been Pwned |
|---|---|
| Google Alerts is a content change detection and notification service. The service sends emails to the user when it finds new results, which can be for anything such as web pages, newspaper articles, blogs, or scientific research. Analysts can set up a specific search criteria that will allow Google Alerts to notify them of hostile reconnaissance activities, such as any time the name of a government department has been used on social media for example. | Have I Been Pwned is a tool that allows analysts to create alerts about the latest known instances of login credential breaches, as part of the Compromise Research use case. Analysts can register entire domains here in order to receive alerts on a vast number of email addresses, providing that they can prove ownership of the domain. |

## Communities

**Cyber-security Information Sharing Partnership (CiSP)** is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

There have been previous instances of government departments alerting the community to instances of Compromise Research. However, this community is not being utilised as much as it should with regards to Digital Risk and Intelligence. If occurrences of compromise research or information leakage have been identified, government departments should be contacted directly, and then posting the information to CiSP to notify all other departments of the event.

## Searching and Scraping Tools

| Google Hacking | GitHub | Domain Permutations | Twitter API | Misconfiguration Identification | Search for Exposed Sensitive Documentation | Scraping Across Websites |
|---|---|---|---|---|---|---|
| Google Hacking, sometimes referred to as “Google dorking”, are techniques utilised by attackers in gathering information, leveraging advanced Google searching techniques. DR&I teams can utilise Google Hacking to identify exposed areas of their digital footprint.<br>This includes searching for security vulnerabilities in web applications, or leaked information in the public domain – using terms such as “Home Office” AND “Strategy OR Staffing” filetype:pdf<br>The Google hacking database provides an excellent overview of what can be searched. | Exposed data on GitHub is increasingly becoming an issue for organisations. Many government code repositories are hosted and publicly available on GitHub. Analysts can now search company name and identifiers across their repositories, in order to understand and identify if crucial IT infrastructure is being exposed, such as AWS keys or proprietary code. | The internationalized domain name (IDN) homograph attack is a way a threat actor can deceive citizens about what remote system they are communicating with. This is done by creating fake domains with permutations of the characters of the URL.<br>Analysts can detect these domain permutations using tools like DNS Twist, and Phishing Catcher by X0rz. If your team uses Kali Linux, then it may be more appropriate to use URL Crazy to generate different types of domain spoof. | Twitter allows analysts to pull in data from their sources around key terms of interest using their Twitter API. This can help in detecting hostile reconnaissance activities or fake social media accounts, as well as any inadvertent exposure on Twitter. | As part of the Infrastructure Misconfiguration use case, analysts can search for misconfigured databases, servers and devices using tools like Shodan and Censys. They can also check for expiring or expired certificates on their infrastructure with Testssl. | Analysts can use Fingerprinting Organisations with Collected Archives to identify exposed documents and investigate the contents and metadata across GitHub. This can be utilised to identify instances of Information Leakage. | Tools like Scrapy or BeautifulSoup are powerful open source frameworks for extracting data from websites. **Caution:** Scraping across criminal domains or nefarious sites may uncover unlawful actions. Please assess legal guidance before undergoing this – Section 5 and 6 will cover this in more detail. |

*Table 2 - Candidate Quick Wins*

## 4.6 Integrating the Incident Response Plan for Digital Risk Events

Digital risk events will happen, and government departments need to be ready for them. Therefore, a formalised process and escalation criteria needs to be set out and well-understood by the team to prepare for these events. We can define a digital risk event as being any event of which an incident has been identified in external sources, which threatens the security of the government department and its data. The incident response plans for digital risk events need to be integrated into the already established response plans within the threat intelligence function.

These plans should include contact lists for anti-abuse teams at social network companies and Internet Service Providers (ISPs) to arrange the take-down of digital assets, i.e. sensitive information being hosted on Pastebin. There are many vendors offering "takedown" services, so government departments should have an understanding of these vendors so their service can be used when necessary.

Government departments should be ready to contact the NCSC in the event of incident that requires escalation, whilst also making full use of the good practice guidance that the NCSC provides on incident management[9].

Good relationships with the legal team and experts in your department, as well as law enforcement agencies, will assist in guiding the right course of action in escalating events. As discussed in Section 4.4, strong relationships with the Personnel Security teams and Information Security teams will ensure incidents, specifically relating to Employee Footprint and Information Leakage, can be remediated quicker and more effectively.

**RECOMMENDATION 8: This paper recommends that Digital Risk and Intelligence teams set out a response plan for digital risk events and have this integrated into the incident response plans of the wider threat intelligence team. This is so that the team can appropriately prepare for and tackle incidents as they occur.**

[9] https://www.ncsc.gov.uk/incident-management

# 5 Creating an Enabling Environment

## 5.1 Overview

In this section of the paper, we will go through the recommendations that **government departments** should follow to enable a Digital Risk and Intelligence capability to be successful. This section of the paper will provide recommendations to do the following:

- Commission external digital risk exposure assessments of their digital footprint at least once a year, to understand how the footprint is changing over time
- Explore vendor trials to adopt, in order to utilise the tools and services in the market, at low cost, to make use of available capability
- Develop service models which blend vendor and in-house resources to achieve a mature automated response function
- Liaise with the appropriate law enforcement agency, through the department's legal teams, to assist in developing policies for monitoring specific public domains, as well as advising on response plans
- Adopt relevant metrics, specifically measuring the mean-time-to-remediate, to appropriately measure the performance of the capability
- Create an educational awareness campaign to encourage employees to better control their digital footprints

This set of recommendations focuses on the medium-term timescales that will assist in bolstering the capability of the Digital Risk and Intelligence team.

## 5.2 Regular Digital Footprint Assessments

A digital footprint assessment can provide an overview of all information within publicly available domains, and an understanding of potential value the information online could be to a hostile threat actor.

These are sometimes referred to as “point in time” digital footprint assessments. Some in the industry argue that these assessments are not overly useful, due to the fact digital footprints are always changing. However, if this is done on a regular basis, for example half yearly or quarterly, then it can be very useful to see how a digital footprint is changing over time, and it may be possible to use these assessments to quantify success.

In-house Digital Risk and Intelligence capabilities, even with high maturity, are unlikely to have the ability to conduct a full digital footprint map of the entire organisation themselves. Specialists, such as vendors, could conduct an external digital risk exposure assessment which will provide a fresh look at the areas of the digital footprint that the capability might be missing. This can also be useful in identifying areas of weakness, and for reassessing the defined scope of operations for the Digital Risk and Intelligence team.

Before beginning an assessment of this kind, a set of pre-requisites is usually provided to ensure those conducting it are focussing their efforts in the correct places. For government departments this will likely consist of the digital assets and points of exposure that they have defined when standing up the capability, as seen in Section 3. This list of pre-requisites can also include areas of their digital footprint that the capability doesn't currently monitor, to assess if the area should be included as part of their scope.

**RECOMMENDATION 9: This paper recommends that government departments commission specialists to provide an external, in-depth digital risk exposure assessment of their digital footprint. This can be done on a regular basis to understand how their footprint is changing.**

## 5.3 Utilising Vendor Trials

The market for tooling around Digital Risk and Intelligence has been described as relatively immature, due to the fact it is still a growing and emerging area of specialism (9). Through our research we have identified that there are a large number of vendors that offer trials of their services and tools, with no long term financial commitment.

Many of these trials can offer a significant amount of capability to the customer for a distinct period of time. This means that government departments can utilise this capability without a long term financial constraint, in order to better assess their digital footprint.

Some of these tools offer the ability to map vast areas of the digital footprint, which is something that can be very difficult to do without the necessary tools. These vendor solutions can offer quick realisation of benefits compared to building in-house tools and can easily exceed that of open source tooling. This is an opportunity to make the most of vendor trials before making the necessary investments into permanent tooling, that will eventually bolster in-house capability.

There is further benefit in this recommendation, as it is an opportunity for the department to assess and explore the tools as a proof of concept. There are many different tools on the market and so it's beneficial to trial and test a number of different tools through their trials to understand the kind of tool that fits best with their organisation and their scope of operations. This will allow government departments the chance to understand what tool they should formally procure in the future.

As the capability matures, government departments should be looking to formally procure a Digital Risk and Intelligence managed service or tool from a vendor which will automate a large portion of their capability to ensure it is significantly more mature, and can appropriately map and control the digital footprint of the organisation.

**RECOMMENDATION 10: This paper recommends that government departments utilise the ad-hoc vendor trials that are available in the immature market in order to make the most of the capability, to better control the digital footprint of the organisation, before making the necessary investments into permanent tooling. Government departments should also do so to understand what tool would be the best fit and should be procured in the future.**

## 5.4 Developing Service Models

Although there is an immature market for Digital Risk and Intelligence vendors, tooling exists that can dramatically increase the ability to monitor digital footprints, particularly for creating automated alerts to specific digital risk events (10). Cost is however an issue and some services and tools can be outside of the department's budget.

We expect that many government departments will need to procure a tool or service at some point in the future, in order to appropriately manage the increasing threat of a growing digital footprint. However, government departments need to be cautious in investing in services, to make sure what they do eventually procure is the right fit for their organisation.

From our engagement research, we learnt that the general consensus of more mature departments, such as GDS or Bank of England, was that when adopting a vendor's tool or service they should ensure that whatever service is being offered, cannot be done by open source tooling. Government departments need to make the most of open source tooling and in-house capabilities before formally procuring a tool or service.

The end result for a mature Digital Risk and Intelligence capability is to have a blend of vendor and in-house resources, so that an automated response to digital risk events can be achieved. For departments that wish to have a capability of higher maturity, and to procure a tool or service, this should be the most cost-effective approach.

**RECOMMENDATION 11: This paper recommends that government departments should aspire to develop a service model, specific to Digital Risk and Intelligence, that blend vendor and in-house resources to achieve a mature automated response function.**

### 5.4.1 Outsourced MSPs

Some government departments have an outsourced Cyber Security Operations Centre (CSOC) and/or Threat Intelligence function. If this is the case, then there is a straight-forward way of creating a Digital Risk and Intelligence capability if one does not currently exist.

From our research engagements, we understood that the reason the capability might not exist for a department with an outsourced CSOC is because the supplier is **not currently being asked** to monitor and map the organisation's digital footprint or cover off the use cases defined within the scope of this paper. To rectify this and mature some form of capability the third-party supplier will need to be requested to undertake some amount of work in monitoring and controlling the digital footprint of the organisation. This will need to be done through a contract change.

**RECOMMENDATION 12: This paper recommends that, if the entirety of the CSOC function is outsourced to a third-party supplier, a contractual change or adjustment should be made to advise the third-party supplier to start monitoring the digital footprint of the government department.**

## 5.5 Metrics

Most of the organisations we engaged with did not have any metrics for their Digital Risk and Intelligence activities, either due to a difficulty in identifying metrics of value or the metrics in general not being suitable. However, the correct metrics can provide a measurement of performance to help drive improvements and can also evidence the Return on Security Investment (ROSI) to senior managers within the organisation, helping to build the argument for further investment (financial and time) in your people and tools.

Metrics, or Key Performance Indicators (KPIs), are particularly difficult to define within this capability, and may need to be tailored to each individual government department. Fundamentally, there needs to be tangible ways of evaluating the efforts the team is putting into developing the capability.

Mean-time-to-remediate (MTTR) (11) is increasingly becoming a widely used metric for Digital Risk and Intelligence. MTTR is a made up of three main components:

- Time to identify
- Time to understand and validate the incident
- Time to rectify the threat

In reducing the average time of these components, your organisation can measure the performance of the capability.

As we learnt from our engagement with Forrester, they hold MTTR up as the best metric currently being used for Digital Risk and Intelligence activities and could be standardised across the industry.

**RECOMMENDATION 13: This paper recommends that Digital Risk and Intelligence teams adopt relevant metrics, specifically measuring the mean-time-to-remediate, to appropriately measure the performance of the capability.**

## 5.6 Law Enforcement Agency Guidance

When it comes to monitoring public domains, websites and platforms for threats, many departments have concerns around acting within the law (for example, when taking down a series of sensitive documentation from a threat actor forum or scraping social media websites for hostile reconnaissance activities).

For some government departments, monitoring the dark web for threats would be very useful. Monitoring the dark web will allow government departments to identify hostile reconnaissance activities at a much earlier stage. They will also be able to search for instances of Compromise Research and Information Leakage, so that the threat of further attack can be stopped at the earliest opportunity. Other departments have very little need for any form of dark web monitoring and doing so would not be a good use of time and resources.

As part of our research, we identified that some government departments are doing some successful work in monitoring the dark web and social media, however others were not comfortable in getting involved in monitoring these areas. The reason for these concerns lies in the fact that many of their security teams do not want to commit any unlawful actions in accessing the dark web or breaching the terms and conditions of the social media websites.

Many law enforcement agencies carry out varying levels of monitoring of the public domain for investigative reasons. These law enforcement agencies will have an in-depth understanding of the logistics of safely monitoring these external sources, like the dark web, and social media sites. For that reason, we believe it would be beneficial for government departments to liaise with an appropriate law enforcement agency for them to provide very straightforward information on exactly how to carry out passive monitoring without committing unlawful actions. The best way to make the most out of this contact would be to do so through your department's legal teams. The legal teams should liaise with the law enforcement contact to ensure the necessary guidance is requested and suitably interpreted for the Digital Risk and Intelligence teams.

It would also be beneficial for government departments to have a contact for which they can query law enforcement questions with regards to threats that have been identified within their digital footprint. From this, government departments will be able to define their own structured policy for Digital Risk and Intelligence.

Some government departments will have a requirement for more detailed monitoring of dark web services than other departments. For some departments, a dark web scraping tool that searches within a set criteria, could be a suitable solution.

It is not necessary for government departments to create fake profiles to access dark web forums or marketplaces as part of their monitoring activities[10].

Government departments should note that there is a duty of care for those analysts who are monitoring the dark web and criminal forums, for the wellbeing of the analysts. This should be taken into consideration and discussed with the law enforcement contact. There is a chance that analysts will come across illegal activity or images, not related to their organisation. This will still require reporting to the appropriate law enforcement agency, and preparation for these instances should be included into a response plan, discussed in Section 4.

There is the need for legal guidance as well, on how a government department should be monitoring certain public domains, and this is addressed in the recommendations to Cross-Government Functions in Section 6.

**RECOMMENDATION 14: This paper recommends that government departments liaise with an appropriate law enforcement agency contact, through their legal teams, who should be able to advise on how to safely and securely conduct passive monitoring of external sources, as well as assisting with law enforcement-based queries.**

[10] Government departments must in no way break the Computer Misuse Act 1990.

## 5.7 Employee Footprint Campaign

Employee Footprint is one of the key use cases in scope of our definition of Digital Risk and Intelligence. Some employees have a great deal of access to sites, information or assets, and therefore they need to be vigilant as their digital footprints could be of particular interest to those with malicious intent, such as criminals, violent protest groups and terrorist groups. They also may unknowingly release too much information online.

This paper **does not** advise that government departments closely monitor the digital footprint of their employees or invade their privacy. The most widely-used solution to this increasing problem is for an organisation to actively encourage their employees to take control and responsibility of their own digital footprint. For this, government departments should create a communications campaign for employees to highlight the importance of protecting and controlling their digital footprints. Organisations like the Centre for Protection of National Infrastructure (CPNI) have developed cross-government materials in order assist departments in curating this campaign (12), such as the “My Digital Footprint” Campaign. This documentation can easily be used to create a campaign.

**RECOMMENDATION 15: This paper recommends that government departments create a communications campaign in order to encourage employees to take better control of their personal and professional digital footprint, in order to better control accidental leakage of information.**

# 6 Leveraging Central Government

## 6.1 Overview

In this section, we will go through the recommendations aimed at **cross-government functions,** such as the NCSC, Government Digital Service, Government Legal Profession and Crown Commercial Service. These recommendations will enable government departments to successfully monitor and control their digital footprint. This section of the paper will provide recommendations for cross-government functions to do the following:

- Searching for sensitive documentation, on behalf of government departments
- Providing legal guidance to government departments enabling them to lawfully search over publicly available domains
- Assessing the possibility of Government-as-a-Platform services
- Recommending commercial mechanisms to government departments for procuring vendor trials, and managed services
- Developing the profession to ensure there is a pipeline of highly trained individuals

## 6.2 Searching for Sensitive Documentation

As government departments each develop Digital Risk and Intelligence capabilities, there is the expectation that some level of duplication of work between departments will occur. It is in the interest of all government departments to reduce this. A key example of this would be the Information Leakage use case. One mitigation technique would be to search over the open web, deep web and dark web for protective marking, such as "OFFICIAL-SENSITIVE". This is a straightforward way of identifying internal sensitive documentation that has been leaked. Security classification is standardised across government departments and not specifically tailored. If many departments start searching for the same criteria of protective monitoring, there is the possibility that these departments will be all searching over the same domain, for very similar criteria.

Following our engagement research, we identified that some government departments have a capability that allows them to search for protective marking and identify instances of Information Leakage, sometimes for that of another government department. In these instances, they will notify that government department to inform them of the possible breach.

With the aim to reduce duplication of work between government departments, it would be reasonable for a cross-government function to take ownership of searching for protective marking across the internet, on behalf of the individual departments. One cross-government function such as the NCSC or Government Digital Service (GDS) should be designated with the responsibility of searching over the public domain for protective marking, on behalf of the government departments, and notifying the breached department.

.

**RECOMMENDATION 16: This paper recommends that the Cabinet Office defines an accountable cross-government function, such as the NCSC, with guidance from GDS, to be designated with the responsibility of committing high level searching over the open web, deep web and dark web for protective marking on documents from across all government departments.**

## 6.3 Legal Guidance and Support

As discussed in Section 5, some government departments would benefit from some level of monitoring of the dark web. Hostile reconnaissance activities also take place on social networking websites. However, the terms and conditions of these websites can regularly change around what data can be extracted.

Our engagement research identified that for some government departments, a barrier to carrying out Digital Risk and Intelligence activities on the dark web and social media services, is the fear of committing unlawful actions in accessing nefarious sites or breaching the terms and conditions of the social media websites.

It became clear through research that government departments are in need of high-level legal guidance that can be used to inform the Digital Risk and Intelligence teams of how to passively monitor these public domains without committing unlawful actions. This can be paired with the guidance provided by the law enforcement agencies from the recommendation in Section 5.5, to ensure that teams are enabled to confidently search all necessary domains, whilst being protected legally to monitor dark web and social media.

**RECOMMENDATION 17: This paper recommends that the Cabinet Office, supported by the NCA, NCSC and Government Legal Profession, should provide suitable legal guidance to DR&I teams and their legal departments to enable them to appropriately, safely and confidently monitor the dark web and social media for threats to their organisation, within their digital footprint.**

## 6.4 Commercial Mechanisms

From our engagement research with government departments who have investigated adopting low cost trials from vendors, it was clear that it is not easy to consume these on a regular basis. We identified that if government departments will be doing this on a more frequent basis specifically in this area, then it would benefit all departments if a cross-government function could develop commercial mechanisms to assist in the adoption of those vendor trials with no long term financial commitment. There is currently a lack of well-developed commercial methodology for departments to adopt when it comes to vendor trials.

If government departments can more easily adopt the services, then this will dramatically bolster in-house capabilities, and improve the cost effectiveness of government wide capabilities.

**RECOMMENDATION 18: This paper recommends that Crown Commercial Service develops and establishes commercial mechanisms that can be adopted by government departments**

**to assist in engaging with Digital Risk and Intelligence vendors that will bolster in-house capabilities in adopting low cost vendor trials.**

## 6.5 Supporting Cross-Department Communities

As government departments each try to develop and mature their own Digital Risk and Intelligence capability, there is the opportunity to collaborate in these capabilities, and share good practice between departments.

Many of the organisations we engaged with attend Cross-Government Working Groups for CTI and/or Security Monitoring. These groups provide an opportunity to update the community on developments at each organisation, and to share best practice. We would strongly recommend the incorporation of digital footprint mapping activities either into an existing group, or alternatively the establishment of a new group focused on Digital Risk and Intelligence. If cross-government functions can pull together the appropriate working groups to act as a forum for departments to discuss digital footprint mapping activities, then each department would benefit immensely from sharing their experiences with other departments who are trying to do the same. They will benefit from understanding what level of maturity the other departments are at, and what steps are being taken to improve the capability.

As mentioned earlier in this paper, the market for Digital Risk and Intelligence vendors is relatively immature (9) and new solutions and tools are being developed very rapidly. As these new tools are being offered, it would be beneficial for cross-government functions to assess the possibility of these services being procured and utilised for cross-departmental use. This would mean that these functions could procure the services once for all departments, as opposed to numerous departments procuring the same service, thus being a dramatically more cost-effective approach to the rapidly changing market.

It would also be beneficial to investigate the incorporation of Digital Risk and Intelligence activities into the NCSC’s Active Cyber Defence (ACD) programme. The ACD programme has been developed with the intension of tackling, in a relatively automated way, a significant proportion of the cyber-attacks that hit the UK. As Digital Risk and Intelligence becomes more of concern for government departments, this paper recommends that the NCSC looks to incorporate automated Digital Risk and Intelligence activities.

**RECOMMENDATION 19: This paper recommends that the NCSC should support cross-department communities through creating working-groups, community building and evaluating the possibility of Government-As-A-Platform (GaaP) for Digital Risk and Intelligence opportunities as the market matures, possibly as part of the ACD programme.**

### 6.5.1 Cluster Security Units

As part of the Transforming Government Security Programme (TGSP), a common Target Operating Model (TOM) is being developed and implemented across the four Cluster Security Units (CSUs)[11]. Led by the Government Security Group (GSG), this will assist in developing a common security framework and profession to support all of Government in meeting the minimum level of security. Each CSU is responsible for defining a set of security service offerings that can then be adopted and rolled out by all CSUs to their customer.

Currently, these service offerings are more generally focused on physical security, with plans to explore a full cyber catalogue in future. We recommend that Digital Risk and Intelligence should be considered for any future cyber security offerings designed by the CSUs, as this is a suitable existing mechanism to define good practice and roll out the capability across a large number of departments.

As they become further developed, the CSUs should aspire to take on increasing levels of Digital Risk and Intelligence activities, on behalf of the separate departments, in order to centralise some of the capabilities, and to reduce any duplication of work in a more cost-effective manner. An example of this could be allowing CSUs to commission digital footprint maps of each of the departments in the Cluster, which could provide a greater understanding of the varying threats to different sized departments.

**RECOMMENDATION 20: This paper recommends that when defining the full cyber catalogue, GSG should include Digital Risk and Intelligence as a security service offering from the CSUs**.

## 6.6 Refreshing Campaign Material

Following the Recommendation 15 in Section 5, cross-government functions, such as Centre for the Protection of National Infrastructure (CPNI), should ensure that the source material that government departments are using, like the “My Digital Footprint” content, is refreshed on a regular basis and therefore can be of most value to departments who are running the campaigns.

As threats to employee digital footprints change over time, cross-government functions should change the source material to reflect this, to ensure that content does not become outdated.

**RECOMMENDATION 21: This paper recommends that CPNI should regularly refresh employee footprint campaign material to ensure it is up to date, and of most value to government departments.**

## 6.7 Development of the Profession

A cyber security skills gap currently exists within the UK’s Critical National Infrastructure (CNI), which includes government as one of its thirteen sectors. This gap is described within the Joint Committee

[11] Cluster 1 is led by HM Revenue and Customs (HMRC); Cluster 2 is led by the Home Office (HO); Cluster 3 is led by the Department for Work and Pensions (DWP); and Cluster 4 is jointly led by the Ministry of Defence (MOD) and the Foreign and Commonwealth Office (FCO).

on the National Security Strategy's Second Report of Session 2017-19 (13) as being predominantly caused by a scarcity of individuals who have the required skills, an inability to match highly competitive reward packages offered by the private sector, and a lack of gender diversity that limits the size of the talent pool.

This struggle to recruit cyber security staff was echoed by the organisations we engaged with, particularly for specialist roles such as open source intelligence analysts. Staff retention is also an issue faced by many organisations. Research by the Cyentia Institute (15) found that 1 in 4 SOC analysts are dissatisfied with their job, while 1 in 3 are actively looking for other job opportunities. One of the reasons cited was a disconnect between expectations of working in a SOC and the day-to-day reality, with examples such as unclear career paths and tedious or repetitive duties.

**Objectives for the Profession**

The DCMS consultation's proposed objectives for the profession to deliver by 2021 are:

- ➢ Professional Development (e.g. Royal Chartered status)
- ➢ Professional Ethics
- ➢ Thought Leadership and Influence
- ➢ Outreach and Diversity
- ➢ Developing the Next Generation

Work is being carried out by the government to ensure the existence of a pipeline of talented individuals.

### 6.7.1 UK Cyber Security Council

In July 2018, the Department for Digital, Culture, Media and Sport (DCMS) launched a consultation on the development of the cyber security profession in the UK (16). The definition of cyber security taken by DCMS is the 19 draft Knowledge Areas from the Cyber Security Body of Knowledge (CyBOK), currently being developed by UK academics led by Bristol University (17).

Delivery of these objectives would be driven by a new and independent UK Cyber Security Council. The consultation closed in August 2018, and in December 2018 DCMS issued a Request for Proposal for the design and delivery of this council (18). Applications are due in February 2019, with work aiming to commence in May 2019.

This paper recommends that Digital Risk and Intelligence teams across government take any available opportunity to be part of the conversation for both the development of the CyBOK and of the UK Cyber Security Council, with the aim to ensure that Digital Risk and Intelligence is appropriately represented as a distinct capability within the Cyber Security Profession.

**RECOMMENDATION 22: This paper recommends that teams developing the CyBOK and the UK Cyber Security Council should review this paper and adopt our recommendations to ensure that Digital Risk and Intelligence is recognised as a beneficial capability.**

### 6.7.2 The Government Security Profession Unit

The Government Security Profession Unit (GSPU) brings together all security professionals working in government to help them gain the skills and knowledge they need to carry out their roles (19). This paper recommends further engagement with GSPU to discuss potential ideas for developing Digital Risk and Intelligence as a profession across government, including:

- Defining standard role profiles and expectations to aid with recruitment;
- Piloting a Digital Risk and Intelligence coaching and/or secondments of skilled DR&I analysts between departments for Learning and Development purposes;
- Evaluating and recommending specific training, qualifications, and certifications.

**RECOMMENDATION 23: This paper recommends that Digital Risk and Intelligence analysts working across government should actively engage with GSPU to provide ideas and solutions for developing the profession.**

# 7 Conclusion

As digital footprints get larger, more complex and therefore of more concern, Digital Risk and Intelligence capabilities are expected to become part of every threat intelligence team.

The National Cyber Security Strategy states that "The UK will be a hard target for all forms of aggression in cyberspace". In achieving that, government departments need to recognise as more information and data is put online as, some of this information could be of significant value to hostile threat actors, thus making it easier for threat actors to plan and commit attacks

In researching this problem, we have held 21 engagements across 14 different organisations, including the NCSC, 5 government departments, 3 cross-government functions, 1 university and 5 commercial partners to understand the current capability within the industry, as well as helping to influence the creation of a Capability Maturity Model.

**This paper provides recommendations as to how government departments can better understand and control their digital footprint through developing and maturing Digital Risk and Intelligence capabilities.**

Firstly, before adopting any of the paper's recommendations, government departments need to **assess their current capability**. This is a crucial starting point for any organisation that wishes to control and manage their digital footprint. Assessing your current capability can be done through using the Capability Maturity Model supplied in Section 3. After assessing at which level your organisation sits, it is recommended that a roadmap is created on how your organisation will reach the aspired level of maturity. At that point, this paper's recommendations can be adopted.

### Short Term Recommendations at the Threat Intelligence Team Level in Mobilising a Digital Risk and Intelligence Capability

These recommendations should allow a government department to build and develop a Digital Risk and Intelligence capability as part of their existing teams.

- Appoint a DR&I team lead, most likely from the cyber threat intelligence team, who can dedicate time to DR&I activities
- Define the scope of the DR&I capability, and a team charter, to ensure the appropriate areas of the footprint will be focused on
- Adopt a series of low cost, publicly available tools as Quick Wins, to easily manage the digital footprint of your organisation
- Engage with senior business leaders to build an understanding of the necessary business context and knowledge for the capability to prioritise important areas of the digital footprint, to determine which use cases are of most value
- Integrate DR&I as part of the response plans already established, so that teams can appropriately prepare for and tackle incidents as they occur

In adopting these recommendations, threat intelligence teams will be able to create an initial operating capability, which will make a sufficient start in managing and controlling the digital footprint of the organisation.

## Medium Term Recommendations at the Government Department Level, in Enabling DR&I Teams

With just the short-term recommendations, government departments are at risk of missing key enablers that will suitably bolster the new capability. For this reason, we have provided the following recommendations to government departments to progress and enable their capability, at a medium-term time frame. This paper recommends that government departments:

- Commission external digital risk exposure assessments of their digital footprint at least once a year, to understand how the footprint is changing over time
- Explore vendor trials to adopt, in order to utilise the tools and services in the market, at low cost, to make use of available capability
- Develop service models which blend vendor and in-house resources to achieve a mature automated response function
- Liaise with the appropriate law enforcement agency, through the department's legal teams, to assist in developing policies for monitoring specific public domains, as well as advising on response plans
- Adopt relevant metrics, specifically measuring the mean-time-to-remediate, to appropriately measure the performance of the capability
- Create an educational awareness campaign to communicate to employees to encourage better control of their digital footprints

## Longer Term Recommendations at the Cross-Government Function Level

Protecting digital footprints for the future will require support from wider organisations in HM Government. To make the most of the expertise available, this paper has made recommendations to **cross-government functions,** such as the NCSC, Government Digital Service, Government Legal Profession and Crown Commercial Service. These recommendations will enable government departments to successfully monitor and control their digital footprint. This section of the paper will provide recommendations for cross-government functions in the following areas:

- The Cabinet Office should define an accountable cross-government function, such as the NCSC with guidance from GDS, to commit high level searching over the open web, deep web and dark web for protective marking on documents from across all government departments
- The Cabinet Office, supported by the NCA, NCSC and Government Legal Profession, should provide clear legal guidance to enable government departments to safely and lawfully monitor public domains
- The Crown Commercial Service should provide clear, reasonable frameworks to assist departments in adopting vendor trials, and eventually procuring managed services

- The NCSC should assess the feasibility of centralising elements of DR&I as part of Active Cyber Defence, and adopting DR&I activities as part of the service offerings from Cluster Security Units
- CPNI should regularly refresh employee footprint campaign material to ensure it is up to date, and of most value to government departments
- Teams developing the CyBOK and the UK Cyber Security Council should review this paper and adopt our recommendations to ensure that Digital Risk and Intelligence is recognised as a beneficial capability
- Digital Risk and Intelligence analysts working across government should actively engage with GSPU to provide ideas and solutions for developing the profession

Supporting government departments and ensuring greater cohesiveness between departments will allow Digital Risk and Intelligence capabilities to adapt to the ever-changing threats to their external facing infrastructures.

Digital footprints are widely understood in the industry to be creating greater risks as they unstoppably increase in size and complexity. It is crucial that government departments make the appropriate investment and changes across CTI functions, departments, and cross-government functions which will fundamentally lead to improvement in the collective security of government information and infrastructure.

# 8 Appendices

## 8.1 Appendix I – Contributors

The authors would like to thank the following organisations for their contribution to this report:

- BAE Systems Applied Intelligence
- Bank of England
- BT
- Cabinet Office
- Cluster Security Unit 2
- Department for Work and Pensions
- Digital Shadows
- Foreign and Commonwealth Office
- Forrester
- Threat Intelligence Team, Government Digital Service
- Threat Intelligence and Counter Fraud, Identity Standards and Fraud, Government Digital Service
- Government Legal Profession
- HM Revenue and Customs
- Home Office
- National Cyber Security Centre
- Transport for London
- University of Warwick

## 8.2 Appendix II – NCSP Funded Publications

This guide has been authored by the Home Office Cyber Security Programme. The authors of this guide are grateful to the Cabinet Office for providing funding for this project from the National Cyber Security Programme (NCSP).

This guide is one of three documents being published as part of NCSP funded projects, each of which are mutually complementary. They are as follows:

- Cyber Threat Intelligence – A Guide for Decision Makers and Analysts
- Detecting the Unknown – A Guide to Threat Hunting
- Controlling Your Exposure – A Guide to Digital Risk and Intelligence

### 8.2.1 Cyber Threat Intelligence

Cyber Threat Intelligence is the process of collecting, processing and analysing information regarding adversaries in cyberspace, in order to disseminate actionable threat intelligence, by understanding adversaries' motivations, capability, and modus operandi, to inform cyber security mitigation measures.

This guide provides an overview for UK government departments and organisations on how to deliver a CTI capability. This covers how to set a CTI strategy, what a CTI function should deliver, how that content should be delivered and how to effectively resource a capability.

### 8.2.2 Threat Hunting

Threat Hunting is the proactive, iterative and human-centric identification of cyber threats that are internal to an IT network and have evaded existing security controls.

This guide, produced via a literature review and engagements with public and private sector organisations, provides recommendations for SOCs, government departments, and across HM Government, to detect unknown malicious activity through development of Threat Hunting as both a capability and a profession.

### 8.2.3 Digital Risk and Intelligence

Digital Risk and Intelligence (DR&I) is the process of monitoring, detecting and remediating threats within the public domain, through the control of an organisation's digital footprint.

This paper provides recommendations as to how and why government departments and HM Government as a whole, can better understand and control their digital footprint through developing a Digital Risk and Intelligence capability. Recommendations are provided at three levels; threat intelligence team level, government department level, and cross-government function level. These recommendations are also provided in the context of short, medium and long-term goals.

### 8.2.4 Full Capability Adoption

We recognise that each of these publications recommends dedicated resources and investment for each capability, and in an ideal world, each would stand alone with discrete objectives. However, it is recognised that there are synergies between each which can be utilised to facilitate a more streamlined capability.

Each of the areas covered by these papers cover different elements of MITRE's Cyber Attack Lifecycle:

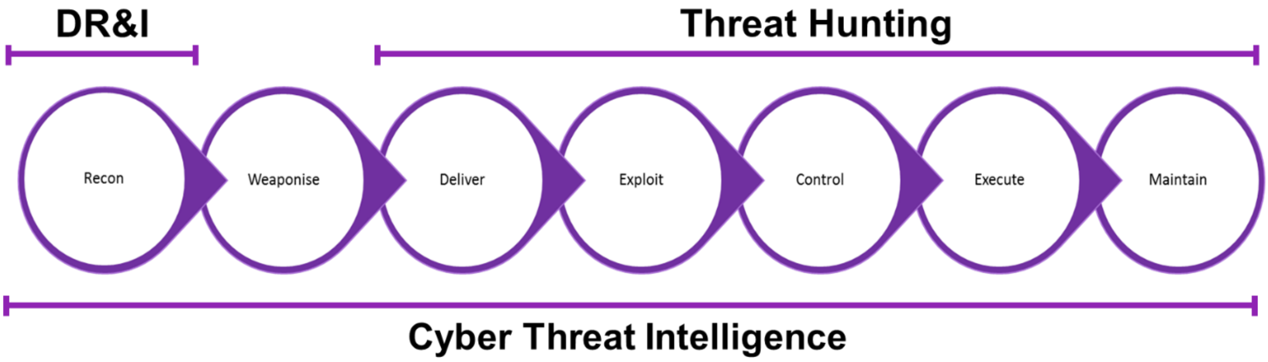


Figure 6 – Capability Scope Comparison

Clearly there are overlaps in the focus of the distinct functions, for example in the reconnaissance phase – whilst CTI and DR&I have different objectives, there is a similarity in content and focus. Depending on business requirements, there may be other areas where further integration can be of benefit, but fundamentally adoption of each capability needs to be based on its cost versus business benefit.

If adopting all three capabilities, we recommend the following considerations be made:

- All three capabilities are subservient to each of the outcomes described in the Minimum Cyber Security Standard. If the minimum standard is not met, it is highly likely that investment in those areas will be more beneficial than these capabilities

- Establishing a mature capability in all three areas represents a significant business investment. Particularly in the public sector, scrutiny of this investment will be high, and we recommend that the business case for each ensures that there is genuine value for money in each area. Each department should prioritise their investment in these capabilities based upon their own requirements and organisational context.

- Access to data and visibility of data is critical to all functions, both internally and externally. We would recommend that the specific pre-requisites for data access in your organisation are understood prior to investment – other organisations consulted have made significant investments, and subsequently failed to realise the benefit due to a lack of data access

- A nascent CTI and Threat Hunting capability should grow together as they have complementary requirements. A mature Threat Hunting capability that has no CTI capability to feed it intelligence will be limited, and likewise a CTI capability feeding information to a CSOC with no threat hunters is likewise limited in value.

For further details on each of these points, please refer to each of the guides specifically.

# 9 Bibliography

1. **NCSC. National Cyber Security Strategy. [Online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf .**

**2. Home Office Cyber Security Programme. *Cyber Threat Intelligence: A Guide for Decision Makers and Analysts .* 2019.**

**3. Lockheed Martin. The Cyber Kill Chain. *Lockheed Martin.* [Online] [Cited: 27 09 2018.] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.**

**4. Barraco, Lauren. [Online] AlienVault, 2014. https://www.alienvault.com/blogs/security-essentials/defend-like-an-attacker-applying-the-cyber-kill-chain.**

5. **MIT Sloan Management Review. *sloanreview.mit.edu.* [Online] 6 March 2017. https://sloanreview.mit.edu/article/to-improve-cybersecurity-think-like-a-hacker/.**

**6. Maryville University. *Online.maryville.edu.* [Online] https://online.maryville.edu/blog/why-top-companies-hire-hackers/.**

**7. Secure Data. *SecureData.com.* [Online] https://www.secdata.com/cybersecurity-and-the-digital-footprint-of-the-hunted/.**

**8. NCSC / Cabinet Office. *Minimum Cyber Security Standard.* London : publishing.service.gov.uk, 2018. Version 0.1.**

**9. Hayes, Nick. *New Tech: Digital Risk Protection, Q2 2018.* s.l. : Forrester, 2018.**

**10. Hayes, Nick. *The Forrester New Wave: Digital Risk Protection, Q3 2018.* s.l. : Forrester, 2018.**

**11. Hayes, Nick. *Assess Your Digital Risk Protection Maturity.* s.l. : Forrester, 2017.**

**12. CPNI. *My Digital Footprint.* s.l. : Centre for the Protection of National Infrastructure (CPNI), 2015.**

**13. Joint Committee on the National Security Strategy. *Cyber Security Skills and the UK's Critical National Infrastructure.* s.l. : House of Lords and House of Commons, 2018.**

**14. Cyentia Institute. *Voice of the Analyst Study.* 2018.**

**15. Department for Digital, Culture, Media & Sport. *Implementing the National Cyber Security Strategy - Developing the Cyber Security Profession in the UK.* 2018.**

**16. The Cyber Security Body of Knowledge. *CyBOK.org.* [Online] https://www.cybok.org/.**

**17. Department for Digital, Culture, Media & Sport. *Request for Proposals - A New UK Cyber Security Council. Annex A - Application Process and Guidance for Applicants.* 2018.**

**18. Government Security Profession. *Gov.UK.* [Online] https://www.gov.uk/government/organisations/government-security-profession.**

**19. Department for Digital, Culture, Media & Sport. *Initial Cyber Security Skills Strategy.* 2018.**