HM Government

Scotland analysis: Security

October 2013

Scotland analysis: Security

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty
October 2013

Cm 8741
£16.00

Any enquiries regarding this publication should be sent to us at: public.enquiries@homeoffice.gsi.gov.uk

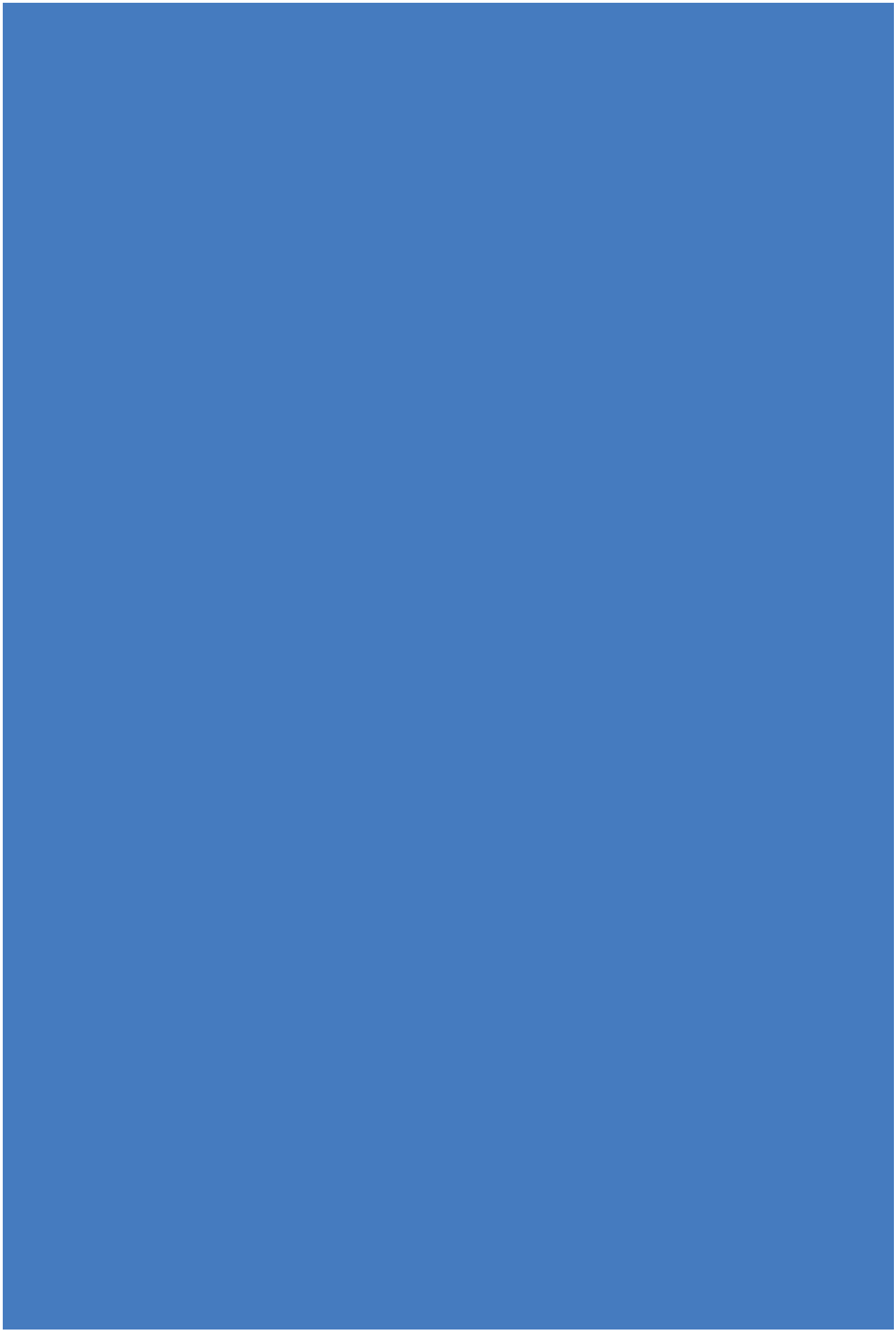
ISBN: 9780101874120

Printed in the UK by
The Stationery Office Limited on behalf of the Controller of Her Majesty's Stationery Office

ID P02599649 10/13 33902 19585

Printed on paper containing 75% recycled fibre content minimum.

Contents



Executive summary

In September 2014 people in Scotland will take one of the most important decisions in the history of both Scotland and the whole of the United Kingdom (UK) – whether to stay in the UK, or leave it and become a new, separate and independent state.

The first duty of any state is the defence of its territory and institutions, and the protection of its citizens and property from harm. In the event of a vote for independence, there would be profound consequences for the defence and security of the UK and an independent Scottish state. The UK Government will ensure that the debate is properly informed by analysis and that the facts that are crucial to considering Scotland's future are set out.

This paper analyses the UK's approach to identifying and managing threats to the national security of the UK, and the implications for these arrangements of a vote for independence. It complements analysis of the UK's approach to defence explored elsewhere in the Scotland analysis series.

It is clearly in the UK's interests to be surrounded by secure and resilient neighbouring countries, including – in the event of a yes vote – an independent Scottish state. While the UK endeavours to work with other countries and international organisations to improve security and fight organised crime for everyone's mutual benefit there is something qualitatively different about being influential and intimately connected with the rest of the UK by being a part of it.

Issues of national security are of the utmost sensitivity, linked to a country's foreign, security and defence policy posture, and any decisions are closely related to matters of sovereignty and democratic accountability. For this reason, a security union is closely connected to the existence of a political union. The creation of an independent Scottish state would see an end to the current arrangements for ensuring Scotland's security, as Scotland, including Police Scotland, would no longer be part of the UK's national security infrastructure and capabilities. In practical terms this means that the present level of strategic and operational communication and co-ordination that occurs everyday across the UK, with Scotland playing a key role within it – whether concerned with counter-terrorism, fighting serious and organised crime or protecting against cyber threats – would end.

National security risks

In May 2010 the UK Government established the UK's National Security Council, and appointed the UK's first National Security Adviser bringing together domestic and overseas security advice. It also developed a strategy to identify the contemporary risks to the UK

and used this to provide a sound basis for making decisions to protect the public. The new strategy, the UK's National Security Strategy (NSS),[1] was published in October 2010.

The UK and other nations face complex national security risks, threats and hazards from a number of sources. These include: international and home-grown threats; cyber attack; a major accident or natural hazard; instability overseas that terrorists can use to exploit and threaten the UK; an increase in the levels of organised crime (which require national and international responses such as narcotics and people trafficking); unconventional attacks using chemical, nuclear or biological weaponry; and threats to border security. Nuclear proliferation is a growing danger and a significant increase in the levels of terrorism relating to Northern Ireland is also identified as a risk. The escalation or realisation of any one of these risks and threats could do grave damage to any nation, including all parts of the UK.

Benefits of the United Kingdom

The Treaty of Union preserved Scotland as a separate legal jurisdiction operating under Scots law. This separate identity has been reinforced by devolution since policing and justice are devolved to the Scottish Parliament. However, national security is reserved[2] to the UK's Government and Parliament at Westminster. Anything that threatens national security affects everyone in the UK. This also means that every effort to increase national security, every penny spent on securing the UK regardless of where it is invested – whether in Aberdeen, Birmingham or overseas – is of direct benefit to the protection of every UK citizen regardless of where they live or work. The UK's security, like its defence, is a common public good from which everyone benefits.

The UK ensures significant benefits in addressing national security risks, for the people and nations of the UK in three broad areas:

a. The role and capabilities of the security and intelligence agencies, the organisations undertaking intelligence analysis, and their relationships with the police and law enforcement agencies, and international partners;[3]

b. UK-wide judicial and police co-operation arrangements that facilitate efforts to tackle serious and organised crime and other offences; and

c. Protective security arrangements including cyber, measures to protect government assets, co-operation on and exchange of sensitive information with other states and organisations, incident response and border security arrangements.

The argument is made that an independent Scottish state would be less at risk. Yet the risks identified in the NSS reveal a wider set of challenges than those related to traditional ideas of conflict between states. Addressing them requires a similarly broad range of policy approaches and capabilities. The UK has built up experience in dealing with these matters over many years. Scotland benefits from these measures to address the risks; risks that will continue to exist – even in altered form – as they do for all Western nations, both large and small, should the referendum lead to the creation of an independent Scottish state. An independent Scottish state would need time to reach the required level of security and in the

[1] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government, 2010, London: The Stationery Office.

[2] *Scotland analysis: Devolution and the implications of Scottish independence*, (CM 8554), HM Government, February 2013, Paragraph 1.11.

[3] Although not directly covered in this paper, it should also be noted that the intelligence and security agencies play a critical role in the UK's defence and foreign policies, and that much of the capability and infrastructure that supports these are integral to the agencies' work on counter-terrorism and against serious and organised crime.

mean time the risk would be of security levels diminishing to the detriment of both Scotland and the continuing UK.

Greater security through integrated UK-wide security and intelligence agencies with global reach

Countering terrorism, espionage[4] and the spread of weapons of mass destruction

Terrorism was identified as being in the highest of four levels of risk (Tier One) in the NSS.[5] It is a live issue which affects states across the world, including countries both large and small here in Europe. Glasgow Airport was subject to a terrorist attack in June 2007. In 2010 in Denmark a plot was discovered which aimed to attack the offices of the Jyllands-Posten newspaper. In the same year an Islamist carried out a bomb attack in Stockholm: a man was later convicted in Scotland for helping to fund it. Norway suffered the effects of extreme right wing ideology with the massacre at Utoya in July 2011. The threat of spying (espionage) did not end with the collapse of Soviet communism: the UK remains a high priority espionage target with the added complication since the Cold War era of the development of espionage in cyberspace. The UK's security and intelligence agencies – the Security Service (MI5), the Secret Intelligence Service (SIS, often known as MI6), and Government Communications Headquarters (GCHQ) – together with the UK's intelligence analysis capability, help protect the UK from these threats. Scotland therefore benefits from a combination of devolved policing and a distinct legal system with access to the full spectrum of capabilities available to the security and intelligence agencies – domestic and overseas, human and technological.

Intelligence unplugged

The first Scotland analysis paper, *Devolution and the implications of Scottish independence*, made clear that all of the current powers and responsibilities of the UK in Scotland would become the responsibility of a new independent Scottish state; and this would include security, defence and intelligence. The continuing UK would not therefore be in a position to protect Scottish interests as it does presently. Scotland would be a separate state. It could not 'share' the UK's security and intelligence agencies for reasons of sovereignty and democratic accountability. They would instead continue to operate in the national interest of the continuing UK. While Police Scotland would be a very important partner for law enforcement in the continuing UK, of course it would lose automatic access to the capabilities and resources of MI5, SIS and GCHQ and the UK's wider intelligence analysis capabilities – information, technology, processes, people and partnerships.

An independent Scottish state would have to build up its own infrastructure because new capabilities would be required. Assuming costs would have to be met from within the Scottish Government's proposed budget of £2.5 billion per year for both defence and security,[6] this compares unfavourably with UK spending of around £33 billion for defence, and over £2 billion per year for the security and intelligence agencies and the National Cyber Security Programme.

---

4 Espionage is a process involving human sources or technical means to obtain information which is not normally publically available. It may also involve seeking to influence decision makers and opinion-formers to benefit the interests of a foreign power.

5 See Chapter One on national security risks to the UK.

6 SNP resolution on NATO, published in full in The Scotsman on 16 July 2012 http://www.scotsman.com/news/politics/top-stories/in-full-snp-resolution-on-nato-1-2414919 retrieved 13 August 2013.

The 'Five-Eyes' community and the rules of intelligence sharing

The UK could not share secret intelligence with an independent Scottish state that had been passed to it by another country without the originator's consent. This is known as the 'Control Principle' and is a widely accepted and understood norm in all international intelligence sharing relationships. The risk of breaking it is the cessation of intelligence sharing by the originator. It takes time to build this trust and confidence. Other states would only share with an independent Scottish state what it was in their own interests to share.

In international intelligence partnerships, most notably the 'Five-Eyes' community (made up of the UK, US, Australia, Canada and New Zealand), each partner makes a substantial contribution in return for the benefits they receive. There would be no automatic right of entry to the 'Five-Eyes' community for an independent Scottish state. There would have to be a benefit to the other members from an independent Scottish state joining, and it would have to make a unique contribution. An independent Scottish state may not possess the capabilities for this, and any new capabilities would take time to establish. Its track record as a recipient of other countries' intelligence material would have to be weighed up, which could take a number of years.

Intercept and communications data

The UK's interception and communications data capabilities play a critical role in tackling serious crime and threats to national security. These sensitive capabilities are provided on a UK-wide basis. Were an independent Scottish state to be established, Police Scotland would not be guaranteed access to the existing capabilities in the continuing UK. It would take many years and significant expense for an independent Scottish state to build up equivalent capabilities.

Better protected through enhanced justice and policing capabilities and international partnerships to tackle serious and organised crime

Judicial co-operation and the arrest and detention of criminals

Despite different legal systems in Scotland, England and Wales, and Northern Ireland, UK legislation helps ensure that they can work effectively together to deliver justice. This means that an arrest warrant issued in one part of the UK may be executed by the police without judicial intervention in another part of the UK. If Scotland votes for independence and joins the European Union (EU), then these arrangements would be terminated. This is because the applicable legislation – enacted by the UK's Parliament and overseen by the UK's Supreme Court – would cease to apply between the two countries. European Arrest Warrants (EAWs) would then apply between an independent Scottish state and the continuing UK; as they do between the UK and all EU states including with the Republic of Ireland. Under the EAW, 93 days was the average length of time it took to extradite someone from the UK in 2010 where the person did not consent to the surrender. The creation of an independent Scottish state would mean replacing fast and efficient justice and policing arrangements with new processes that are more bureaucratic and take considerably longer to deliver justice than existing UK-wide arrangements.

Major public order events and mutual-aid

Existing powers enable police officers from one part of the UK to operate in any other part of the UK. This enables them to provide support during major disturbances to public order. Mutual aid arrangements during the 2005 G8 Summit in Gleneagles saw police forces from across the UK providing support to their counterparts in Scotland. The 2011 riots in England

saw non-English forces, including from Scotland, lending support to their counterparts in England, and police forces from across the UK were involved in providing support during the 2012 Olympic Games and stand ready to do so again during the 2014 Commonwealth Games in Glasgow. With the creation of an independent Scottish state, in addition to potential growing divergences over time in doctrine, culture and practice, there would also be significant legal impediments. For instance, police officers from the continuing UK and an independent Scottish state would no longer have powers to arrest and detain in each others' jurisdictions. Within the UK, Scotland therefore enjoys the best of both worlds – devolved policing with the support, should they need it, of officers from the rest of the UK.

Fighting serious and organised crime

A significant increase in the level of organised crime is identified in the NSS as a Tier Two risk. While Scotland has an advanced and effective infrastructure to tackle serious and organised crime, the UK's national and international links and wide-ranging capabilities are critical to effectively managing the threat. As with the fight against terrorism, there are significant advantages for Police Scotland and the rest of the UK in such arrangements. These would be undermined by the loss of guaranteed access to intelligence from a range of local, regional and national sources, including the National Crime Agency's Intelligence Hub. Partner status in the UK's established international partnerships, and access to specialist capabilities, would also be at risk with the establishment of an independent Scottish state.

Greater resilience through UK-wide cyber security, and other protective security arrangements

A common approach to cyber security

Hostile attacks upon UK cyberspace by other states and large scale cyber crime is a Tier One risk to the UK. Cyber crime is estimated to cost the UK several billions of pounds per year.[7] In addition to threatening the operation of Government and the electronic delivery of public services, hostile foreign states also seek to acquire information about company activity and to steal intellectual property. The UK's £860 million cyber security programme delivers enhanced cyber security for the benefit of the whole of the UK, strengthening the services the public rely upon and enabling the UK to become a safer place for businesses to operate. The UK leads other G20 countries in its ability to withstand cyber attacks.[8]

An independent Scottish state would no longer be covered by the UK's National Cyber Security Programme. Delivering a successful cyber security programme requires the recruitment and retention of highly skilled and scarce cyber security experts in competition with the private sector, as well as considerable financial investment. An independent Scottish state would require new investment in cyber security infrastructure.

The Scottish security industry

A strong and competitive UK security industry is vital to the UK's national security and in particular to the delivery of the UK's counter-terrorism, cyber-security, serious and organised crime, and defence strategies in the UK and overseas. The UK Government is promoting UK's security industry overseas including through government-to-government contracts

---

7 HM Government (2013), *Serious and Organised Crime Strategy*, (CM 8715) London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf retrieved 07 October 2013.

8 The UK cyber security strategy: Landscape review, National Audit Office, 2013 http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/ which cited research by Booz Allen Hamilton and the Economist Intelligence Unit's 2012 Cyber Power Index.

where it can prioritise UK companies. This is based on the track record built up by the UK on security matters. The continuing UK would no longer represent Scottish business interests as it currently does through its extensive network of overseas posts and trade promotion activities.

Conclusion

The analysis in this paper shows how Scotland benefits from the UK's extensive security and intelligence, law enforcement and protective security machinery – both domestically and overseas – while preserving the distinct Scottish legal system. This constitutional setup brings benefits to all who live in the UK. Investment in national security in any part of the UK and in partnerships overseas delivers benefits to everyone in these islands. In the event of a vote for independence, security bodies that support the UK in its present form would continue to operate on behalf of the continuing UK and would have no legal authority in an independent Scottish state. Scotland would be a separate country. The continuing UK would no longer be responsible for Scotland's security.

While an independent Scottish state and the continuing UK might of course co-operate on issues of mutual interest, geographic proximity and historical relations would not guarantee continued access to the UK's security and intelligence capabilities. International intelligence sharing depends upon making a contribution valued by your partners and on mutual trust, both of which an independent Scottish state would need to establish. Scotland would lose the economies of scale intrinsic to the existing UK-wide arrangements and therefore may have to accept less efficient and effective capabilities. An independent Scottish state in the EU would have to introduce a new – slower and less efficient – regime for cross-border judicial and police co-operation against crime. It would also separate Scotland from the continuing UK's cyber security programmes, and the machinery which promotes UK security exports. In all these areas, Scotland would be exchanging the absolute entitlement it has as part of the UK for increased bureaucracy, greater formality and partial co-operation only when it was in both parties' interests.

Introduction

Why security matters in the debate about independence

Scotland and its people are an integral part of the UK's national security. The UK Government believes that Scotland is better off as part of the UK, and that the UK is stronger, safer and more secure with Scotland as part of it.

The referendum on independence presents one of the most important decision points in both Scotland's and the UK's history. It is important that the debate ahead of the referendum is informed by wider analysis, and that the facts that are crucial to considering Scotland's future are set out.

The onus is on those who want Scotland to leave the UK to set out their proposals for independence and address some of the key questions relating to its implications. Not all of the answers to these questions can be known in advance of the referendum. This is because some of the details can only be established through negotiations between the representatives of an independent Scottish state, the continuing UK, and other bodies, for example the EU, and the North Atlantic Treaty Organisation (NATO). These negotiations would have to take place in the event of a yes vote for Scottish independence and their outcomes would be uncertain for an independent Scottish state.

The objective of the UK Government's Scotland analysis programme is to provide comprehensive and detailed analysis of Scotland's place in the UK and how that would be affected by independence. The outputs of this analysis will provide sources of information and aim to enhance understanding on the key issues relating to the referendum. As such, the programme should be a major contribution to the independence debate.

The scope of this paper

This is the seventh paper in the Scotland analysis series. It presents the UK Government's analysis of the security implications of Scottish independence. It reviews how the current arrangements have resulted in a strong security union between Scotland and the rest of the UK, and examines four key components of the UK's national security:

- The national security risks to the UK;
- Secret intelligence – the role and capabilities of the security and intelligence agencies, those undertaking intelligence analysis, as well as interception and communications data;

- Justice, policing and combating serious and organised crime; and
- Cyber and protective security, and resilience.

An independent Scottish state's national security would of course be affected by its policies on defence, EU and international affairs, and the protection of its borders and immigration. These important factors have been, or will be, addressed elsewhere in the Scotland analysis programme. Although not directly covered in this paper, it should be noted that the intelligence and security agencies play a critical role in the UK's defence and foreign policies, and that much of the capability and infrastructure that supports defence and foreign policy is integral to the agencies' work on countering terrorism and serious crime.

The UK Government's first Scotland analysis paper, *Scotland analysis: Devolution and the implications of independence*, set out that the UK's key national institutions would operate on behalf of the continuing UK as before, but would have no power to act in or on behalf of an independent Scottish state, and would not be under any obligation to create the structures to do so.[1] This would include the UK's security and intelligence agencies, UK-wide law enforcement agencies, cyber security programme, and resilience capabilities and supporting infrastructure.

The government of an independent Scottish state would therefore have to set up many new institutions and establish their security credibility. During that time citizens, businesses, including owners of Critical National Infrastructure, and Police Scotland, as well as other countries and international organisations would be faced with considerable uncertainty.

Assessing the UK and Scottish security positions

This paper considers the national security risks that affect the UK and the extent to which they are shared by other countries around the world – large and small – but particularly in Europe.

The paper considers the extent to which ensuring the security of any one part of the UK delivers the security of all of it, regardless of whether that investment is made in one geographical location or another. The key strengths of the UK's security framework examined in this paper include the role and capabilities of the UK's security and intelligence agencies, as well as those undertaking intelligence analysis; the institutions that facilitate justice and policing co-operation including in combating serious and organised crime; and the institutions and capabilities that facilitate cyber and other forms of protective security, and which ensure the UK's resilience in the face of major events.

The reality for many smaller countries in terms of national security is that even in the absence of a direct threat to their territorial integrity such as a militarily hostile country on their borders, they are no less affected by a range of threats than other, much larger, states. These include terrorism, espionage (spying), and other countries seeking to obtain their intellectual property through traditional and cyber means for commercial and other reasons.

There is a great deal already in the public domain that allows certain conclusions to be drawn. This open source material includes the UK's assessment of national security risks published in October 2010 in the NSS. As long as Scotland remains an integral part of the UK, the NSS's assessments remain applicable to all of the UK and a threat to Scotland would be considered a threat to the rest of the UK and vice versa.

---

[1] *Scotland analysis: Devolution and the implications of Scottish independence*, HM Government, February 2013, page 8.

Furthermore, a number of the risks identified in the NSS have materialised both in the UK and in friendly countries nearby, including those cited by the Scottish Government[2] and independent commentators[3] as comparators on matters of defence and security. These include attempted and successful terrorists attacks, cyber attacks, and the ongoing menace of serious and organised crime including narcotics, people smuggling and child exploitation.

The Scottish National Party (SNP) passed a resolution in 2012 on the foreign, security and defence policies of an independent Scottish state.[4] Excluding defence and foreign policy, the resolution does not discuss security matters in depth. The resolution states "While conventional military threats to Scotland are low, it is important to maintain appropriate security and defence arrangements and capabilities. This includes a cyber security and intelligence infrastructure to deal with new threats and protect key national economic and social infrastructure."

Although the analysis contained in this paper considers some policy options that could be available in the event of a vote for independence, the conclusions do not attempt to anticipate final decisions, some of which could depend on the outcome of political negotiations between representatives of the continuing UK and an independent Scottish state.

Structure of the paper

Chapter 1 sets out the most serious national security risks faced by the UK. It focuses on those engaged with by the UK national security machinery and not covered by other papers in this series such as those already published on defence, and in other parts of the Scotland analysis programme.

Chapter 2 examines the roles and capabilities of the UK's security and intelligence agencies, as well as the organisations undertaking intelligence analysis, and the way they work together with the police and overseas partners to keep the UK safe from terrorism, espionage and the proliferation of weapons of mass destruction. It considers how these capabilities and partnerships might be impacted by a vote for Scottish independence, drawing on the reality of established and accepted practices for international intelligence co-operation. It also sets out the importance of having a common framework for obtaining intercept material and communications data throughout the UK – a capability that underpins much of the work that is undertaken to combat terrorism and serious and organised crime.

Chapter 3 considers how national legal frameworks operating within the UK facilitate rapid judicial and police co-operation to gather evidence and bring suspected criminals and fugitives to justice. It also explores the benefits when combating serious and organised crime of having access to the capabilities and assets of the National Crime Agency, while respecting the devolved nature of policing in Scotland.

Chapter 4 looks at the impact of cyber threats, the importance of cyber security, and the benefits of being a part of a single UK-wide National Cyber Security Programme and how this can help to attract and retain business investment. It also looks at the benefits for Scotland's security industry of being in the UK, in the context of the UK Government's efforts to increase

---

2 Tom Peterkin, SNP prepares to vote on NATO, Scotland on Sunday, 14 October 2012, and Jason Allardyce, Support for solo Scotland waning, The Sunday Times, 27 January 2013 (behind pay wall) http://www.thesundaytimes.co.uk/sto/news/uk_news/scotland/article1202537.ece retrieved August 2013.

3 Malcolm Chalmers, The End of an 'Auld Sang' Defence in an Independent Scotland, RUSI briefing paper, April 2012 http://www.rusi.org/downloads/assets/End_of_an_Auld_Sang.pdf retrieved 13 August 2013.

4 SNP resolution on NATO, published in full in The Scotsman on 16 July 2012 http://www.scotsman.com/news/politics/top-stories/in-full-snp-resolution-on-nato-1-2414919 retrieved 13 August 2013.

security exports. It also considers the benefits of the UK's resilience capabilities in reacting to and recovering from attacks involving chemical, biological, radiological and nuclear (CBRN) materials and the importance of effective border security in preventing dangerous individuals entering the UK or threatening aircraft.

The annexes provide detailed information that supplements the analysis in Chapters 2 and 3.

Chapter 1: National security risks to the United Kingdom

Securing the United Kingdom

1.1 In the UK, national security is reserved to the UK Government and Parliament at Westminster. This is because the UK Government has a duty to act in the name of every UK citizen, to protect both the integrity of the state and their rights and liberties. In order to discharge this responsibility, the UK Government and Parliament – like all successful modern states – retain exclusive rights that only they can exercise. Anything that affects or threatens to undermine national security thereby affects everyone in the UK. It also means that every effort to increase national security, every penny spent on securing the UK regardless of where it is invested is of benefit to the protection of every citizen where ever they live. The UK's security, like the UK's defence, is a common public good from which everyone benefits.

1.2 In 2010 the UK Government took a policy decision to develop a strategy to identify the risks the UK faces today and to use this to provide a sound basis for making policy decisions for the protection of UK citizens. It established the UK's first National Security Council, and appointed the UK's first National Security Adviser.

What are the national security risks to the United Kingdom?

1.3 The UK's National Security Strategy[1] (NSS), published in October 2010, prioritises the most pressing national security risks to the UK in order to identify the actions and resources needed to deliver the UK's responses to those risks. These were prioritised into tiers based on a combination of the likelihood of the risk arising and its potential impact. It identified a number of key risks which provide an important starting point for any consideration of security issues in relation to the creation of an independent Scottish state. Some of the key risks and threats and how far they have materialised during the year leading up to the publication of the 2012 NSS annual report,[2] and the period July 2011 to December 2012 covered by the first annual report[3] on the UK's counter-terrorism strategy,[4] are set out below.

---

1 *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government, 2010, London: The Stationery Office.

2 Annual Report on the National Security Strategy and Strategic Defence and Security Review, Cabinet Office, Nov. 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83775/121128-Annual-Report-to-Parliament-on-NSS-and-SDSR.pdf, retrieved August 2013.

3 Annual Report on CONTEST: *The United Kingdom's Strategy for Countering Terrorism Annual Report*, HM Government (March 2013) London, The Stationery Office.

4 *CONTEST: The United Kingdom Strategy for Countering Terrorism*, HM Government, July 2011, London, The Stationery Office.

TIER ONE RISKS

International terrorism affecting the UK or its interests, including a chemical, biological, radiological or nuclear attack by terrorists; and/or a significant increase in the levels of terrorism relating to Northern Ireland

1.4 In the most recent report on the UK's counter terrorism strategy, published in March 2013, the UK Government stated that the threat to the UK from international terrorism is assessed by the Joint Terrorism Analysis Centre[5] (JTAC) as SUBSTANTIAL.[6] This means that a terrorist attack is a strong possibility and may occur without warning. Al Qa'ida continues to operate around the Afghanistan-Pakistan border and still has the capability to conduct terrorist attacks in the UK and other countries.

1.5 Al Qa'ida affiliates around the world, notably in Yemen and in North and West Africa, have become a greater threat in their own right, operating without reference to the Al Qa'ida leadership, collaborating more closely with each other and taking advantage of regional instability and the breakdown of law and order. The terrorist threat the UK faces is now more diverse than before, dispersed across a wider geographical area and often in areas without effective governance. This poses significant challenges to the UK's national security and to the security and intelligence agencies and departments working on counter-terrorism.

1.6 The terrorist threat to the UK from far right extremism is low in comparison to the threat from international terrorism. Police data shows that in 2012 there were five arrests under terrorism legislation in relation to far right-wing activity.[7] The threat from Northern Ireland Related Terrorism is assessed as SEVERE in Northern Ireland – this means that a terrorist attack is highly likely; and MODERATE in Great Britain – meaning a terrorist attack is possible but not likely.

Hostile attacks upon UK cyber space by other states and large scale cyber crime

1.7 According to the most recent NSS annual report, cyber attacks cost the UK economy billions of pounds a year and pose a significant national security threat. In response, a sustained national programme, now in its delivery phase, is transforming the UK's understanding of the cyber threat and improving its cyber defences in parallel with greater investment from the private sector. As the UK Government's 2013 Serious and Organised Crime Strategy set out, based on the evidence available the costs of cyber crime in the UK are likely to be at least several billions of pounds each year.[8] A survey published by PwC in 2013 found that £35,000 – £65,000 was the average cost to a small business in the UK of their worst security breach of the year.[9]

---

5 The Joint Terrorism Analysis Centre (JTAC) is the UK's centre for all-source analysis and assessment of international terrorism. JTAC sets threat levels, and issues analytical reporting to Government Departments and agencies.

6 Threat levels are designed to give a broad indication of the likelihood of a terrorist attack. These are as follows: Critical – an attack is expected imminently; Severe – an attack is highly likely; Substantial – an attack is a strong possibility; Moderate – an attack is possible, but not likely, and Low – an attack is unlikely.

7 These figures are held by the National Domestic Extremism & Disorder Intelligence Unit (NDEDIU). It was formerly known as the National Domestic Extremism Unit (NDEU) as referenced in the CONTEST Annual Report published March 2013. Annual Report on CONTEST: *The United Kingdom's Strategy for Countering Terrorism Annual Report*, HM Government (March 2013) London, The Stationery Office.

8 *Serious and Organised Crime Strategy*, HM Government, 2013, London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf retrieved 07 October 2013.

9 PWC 2013 Information security breaches survey, Executive Summary. http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf retrieved 01 August 2013.

A major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic

1.8 Severe weather and flooding has occurred in different regions but not to an extent requiring a national response.

TIER TWO RISKS

Risk of major instability, insurgency or civil war overseas which creates an environment that terrorists can exploit to threaten the UK

1.9 Instability overseas, which has the potential to lead to terrorism or conflict affecting the UK, has increased over the year, although not universally. Most of these risks are focused in the Middle East and North Africa, South Asia and the Sahel where a confluence of transnational and internal country risk factors are driving instability.

1.10 The CONTEST annual report states that the uprising in Syria, beginning in early 2011, has involved many organisations with different political views and tactics; some connected with and supported by Al Qa'ida in Iraq. These terrorist groups conducted over 600 attacks in 2012 and, like others associated with Al Qa'ida, continue to attract recruits from the UK and elsewhere in Europe. There are now hundreds of foreign fighters from Europe in Syria. As and when UK residents return from Syria there is a risk that they may carry out attacks using the skills that they have developed overseas.

A significant increase in the level of organised crime affecting the UK

1.11 Serious and organised crime costs the UK more than £24 billion per year[10] and causes a significant proportion of the crime on our streets. There are around 37,000 organised criminals in the UK, linked to approximately 5,500 organised crime groups. Many of these groups are linked to crime syndicates overseas and their activity harms communities in every part of the UK – Scottish Government data indicates that there are more than 4,000 people involved in at least 350 such groups in Scotland.[11]

TIER THREE RISK

A significant increase in the level of terrorists, organised criminals, illegal immigrants and illicit goods trying to cross the UK border to enter the UK

1.12 Regional conflicts (including in Afghanistan, Syria, Libya and Somalia) increase the potential threat to the security of our borders.

International impact of these risks

1.13 These risks do not apply to the UK in isolation. Many states, both large and small, face similar risks – and these have materialised with devastating consequences.

1.14 The impact of the threat from terrorism, for example, has been felt across the world, including in European states close to the UK. 2004 saw the murder of Theo Van Gogh in The Netherlands. Glasgow Airport was subject to a terrorist attack in June 2007. In 2010 in Denmark a plot was discovered which aimed to attack the offices of the Jyllands-Posten newspaper. In the same year an Islamist carried out a bomb attack in Stockholm: a man was later convicted in Scotland for helping to fund it. In 2012 France

[10] *Serious and Organised Crime Strategy*, HM Government, 2013, London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf retrieved 07 October 2013.

[11] *One Year On, Letting Our Communities Flourish: A Strategy for Tackling Serious Organised Crime in Scotland*, The Scottish Government, 2010 Edinburgh, http://www.scotland.gov.uk/Resource/Doc/313639/0099447.pdf retrieved 14 October 2013.

suffered terrorist attacks on the streets of Toulouse. Norway suffered the effects of extreme right wing ideology with the massacre at Utoya in July 2011.

1.15 The same applies to the risk from cyber attacks which impact both large and small countries across the globe. A report published by RAND Europe for the Swedish National Defence College in 2013 noted that, in the last five years, for countries including Canada, Denmark, Estonia, France, The Netherlands, Russian Federation, the UK, and the US (countries for which information was available) the cyber security threat had been prioritised in the top-tier of security issues, according to their national risk assessments.[12]

1.16 In 2007 Estonia suffered a major cyber attack affecting important national infrastructure including banking, telecoms, and the media. More recently major US banks have suffered a series of sophisticated cyber attacks taking down their websites for hours and days at a time.[13] Events of this nature are costly. A survey by Deloitte / EMC in 2013 found that in Ireland €135,000 was the average cost per organisation of a cyber security incident. Cyber crime costs Irish organisations on average 2.7 per cent of their annual turnover. €29,954 was the average clean-up and remediation cost to organisations following an incident.[14]

1.17 Organised criminal groups also continue to operate throughout the world, smuggling drugs, laundering money and trafficking people.[15] The United Nations Office for Drugs and Crime (UNODC) estimates that the annual turnover of transnational organised crime groups and networks is $870 billion.[16] The most significant and sophisticated of these networks now operate in the manner which was previously the preserve of nation states or large corporations. They have access to vast illicit wealth, recruit specialist personnel and seek to wield state-like commercial and political power.[17]

What this means for Scotland

1.18 The risks identified in the NSS, and their manifestation in Western European countries, reveal a wider set of challenges than those related to traditional ideas of conflict between states. Addressing them requires a similarly broad range of policy approaches and capabilities.

1.19 Terrorists, organised criminals and those who conduct cyber attacks have demonstrated that they consider Scottish interests, people, and infrastructure targets for attack. Terrorist groups have demonstrated that they are unconcerned by differences

---

[12] Robinson et al, Cyber-security threat characterisation – A rapid comparative analysis, RAND Europe, 2013 http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.sum.pdf retrieved 03 October 2013.

[13] Joseph Menn, Cyber attacks against banks more severe than most realize, 18 May 2013, Reuters. http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518 retrieved 01 August 2013.

[14] Irish Information Security and Cybercrime Survey 2013, Deloitte / EMC http://www.deloitte.com/assets/Dcom-Ireland/Local%20Assets/Documents/ERS/2013/IE_A_ERS_Cyber%20Crime%20Survey_digi_0713.pdf retrieved 12 August 2013.

[15] UN Office on Drugs and Crime, https://www.unodc.org/unodc/en/organized-crime/index.html retrieved 01 August 2013.

[16] *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organised Crimes*, UN Office on Drugs and Crime (UNODC), 2011 www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf retrieved 07 October 2013.

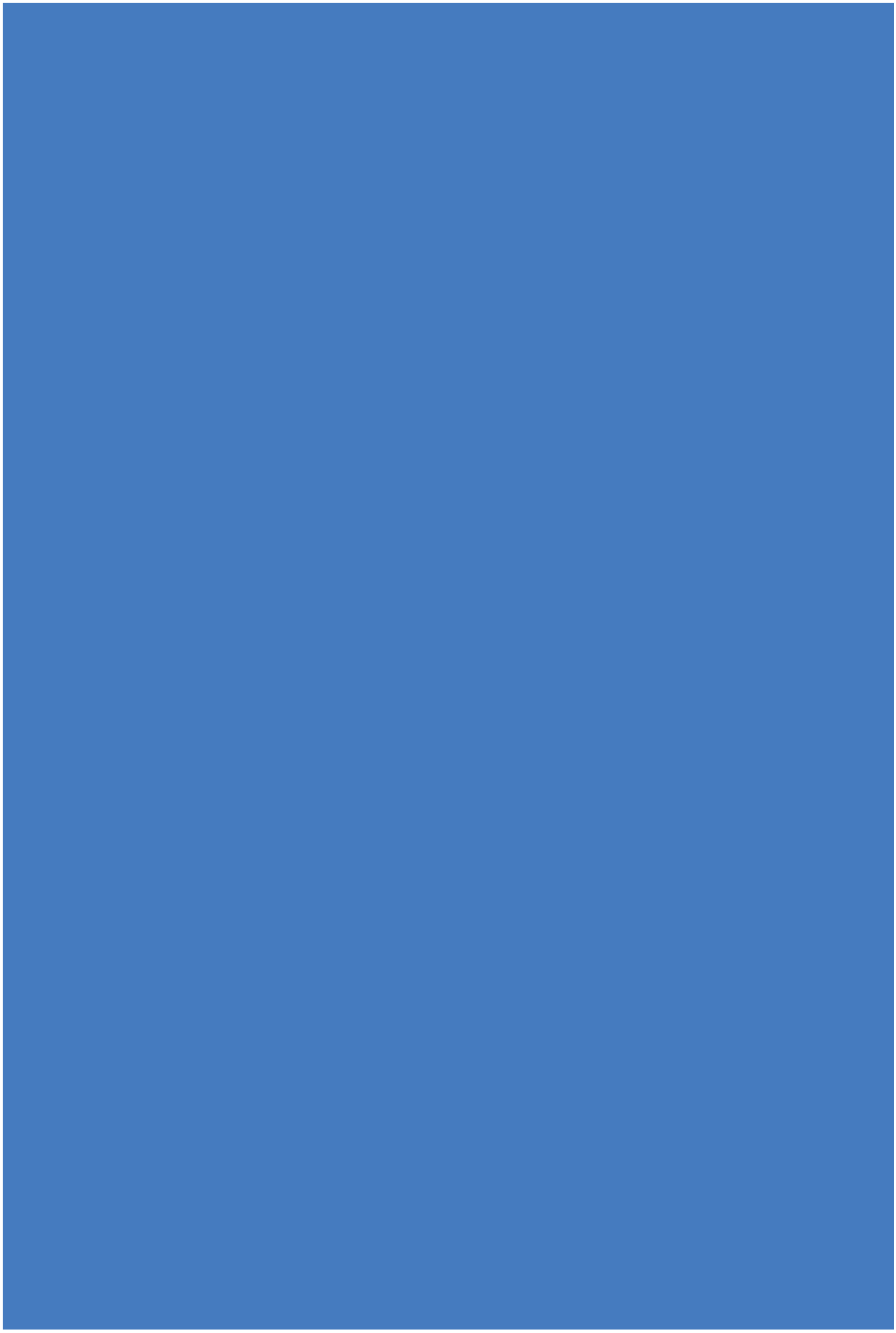
[17] *Serious and Organised Crime Strategy*, HM Government, 2013, London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf retrieved 07 October 2013.

in nationality amongst Western countries; Scottish people suffered directly at the hands of terrorists in Glasgow in June 2007 and the In Amenas attack in Algeria in January 2013. Organised criminals have and will continue to target Scottish people and their interests because the perceived benefits of such crimes remain. The perpetrators of cyber attacks, including cyber espionage, have shown little regard for international boundaries. These threats will persist in the future.

1.20 The creation of an independent Scottish state will, however, without proper planning and investment lead to a reduction in the capability of its government to protect Scottish interests, infrastructure and people from these threats. A reduced capability to tackle a persistent threat would result in an increased risk to the Scottish people. As this paper will illustrate, the UK already possesses extensive capabilities to counter and manage national security threats. The UK has some of the finest security and intelligence agency capabilities in the world, and has developed extensive international partnerships to help tackle cyber activity, organised crime and terrorist threats. The recent launch of the National Crime Agency will provide a strategic overview of organised crime, allowing crime-fighting teams to handle effectively the scale and complexity of the issue. The UK's development of the National Cyber Security Programme led to the Economist Intelligence Unit ranking the UK in 2012 number one amongst the G20 countries in its ability to withstand cyber attacks and to develop a strong digital economy.[18] An independent Scottish state may not have capabilities equivalent to those enjoyed by the UK, leaving the Scottish people exposed to greater risks from these national security threats.

1.21 An independent Scottish state would need to undertake its own national security risk assessment. Its conclusions may differ from the UK's but it is highly unlikely, given the risk, threats and hazards highlighted here that Scotland would continue to face, and the need to mitigate against them. An independent Scottish state would need to determine how it would manage the risks identified. Individual states may articulate their national security risks in different ways, and assign responsibility for mitigating them to differing organisations according to their own national arrangements, but the available options for tackling these risks will remain broadly consistent.

[18] *The Cyber Power Index 2012*, The Economist Intelligence Unit, January 2012, available at: www.cyberhub.com quoted in The UK cyber security strategy: Landscape review, National Audit Office, 2013 http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf retrieved 04 October 2013



Chapter 2: Secret intelligence – the role and capabilities of the UK's security and intelligence agencies

- As a part of the UK, Scotland benefits from the full spectrum of capabilities available to the UK's security and intelligence agencies and organisations responsible for intelligence analysis. These capabilities are used for national security, for the prevention and detection of serious crime and in the interests of the economic well-being of the UK. This includes protecting against terrorism and espionage, supporting the military, and producing secret intelligence to support the UK's defence and international interests.
- Scotland benefits from a sophisticated UK-wide Counter Terrorism (CT) policing model developed since 9/11. Working together, the police and the security and intelligence agencies play distinctive but complementary roles in protecting the UK. This unique relationship is at the core of the highly resilient and successful UK model for countering terrorism.
- The UK's security and intelligence agencies, and organisations responsible for intelligence analysis, work with over 200 partner services around the world. These international partnerships are based on a track record of trust and confidence built over decades, the safeguarding of secrets provided to the UK by other states, as well as in making a substantial contribution in return.
- Overseeing the security and intelligence agencies, and the organisations responsible for intelligence analysis, are independent commissioners, the Investigatory Powers Tribunal and Parliament's own Intelligence and Security Committee, as well as the relevant Secretaries of State. An independent Scottish state would need to create new independent judicial and parliamentary oversight mechanisms.
- Under an independent Scottish state Police Scotland would lose automatic access to the full range of capabilities and technical infrastructure of MI5, SIS and GCHQ.
- The operation of the internationally recognised 'Control Principle' would rule out the UK sharing, with an independent Scottish state, intelligence provided to the UK by a third country without its consent.
- In addition to its effect on countering terrorism, tackling serious crime and support to the military, the loss of such access and capabilities would also impact on an independent Scottish state's ability to counter espionage and hostile foreign intelligence activity which continue to exist in both traditional and cyber forms.

- An independent Scottish state would have to make provision for its own security and intelligence agencies and supporting infrastructure. It would have to establish new overseas intelligence sharing relationships which in turn would rely on an independent Scottish state assuring international partners of the protection of their secrets, as well as its ability to offer something in return.
- Costs would have to be met from within the Scottish Government's proposed budget of £2.5 billion per year for both defence and security. This compares with UK spending of around £33 billion for defence, and over £2 billion per year for the security and intelligence agencies and the National Cyber Security Programme.

Who are the UK's security and intelligence agencies?

2.1 The Security Service (MI5) is responsible for protecting the UK against threats to national security. These include terrorism, espionage,[1] and the proliferation of weapons of mass destruction. It also provides security advice to a range of other organisations. Its role as defined by the Security Service Act 1989 is: to protect national security, and in particular to protect against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means; to safeguard the economic well-being of the UK against threats posed by the actions or intentions of persons outside the British islands; and to act in support of the police and other law enforcement agencies in the prevention and detection of serious crime.[2]

2.2 The Secret Intelligence Service (SIS) operates overseas to collect secret foreign intelligence on issues concerning the UK's vital interests in the fields of security, defence, serious crime, and foreign and economic policies. SIS uses human and technical sources to meet these requirements, as well as liaison with a wide range of foreign intelligence and security services.[3]

2.3 The Government Communications Headquarters (GCHQ) has two main missions: gathering intelligence through the monitoring of communications and providing services and advice as the UK's authority for information security, sometimes known as Information Assurance.[4] GCHQ also includes the National Technical Assistance

[1] Espionage is a process involving human sources or technical means to obtain information which is not normally publically available. It may also involve seeking to influence decision makers and opinion-formers to benefit the interests of a foreign power.

[2] S. 1(a) and (b) of The Security Service Act 1989 states: There shall continue to be a Security Service (in this Act referred to as "the Service") under the authority of the Secretary of State.; and, The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

[3] S.1 of The Intelligence Services Act 1994 states: (1) There shall continue to be a Secret Intelligence Service (in this Act referred to as "the Intelligence Service") under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be—
(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and (b) to perform other tasks relating to the actions or intentions of such persons. (2) The functions of the Intelligence Service shall be exercisable only— (a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or (b) in the interests of the economic well-being of the United Kingdom; or (c)in support of the prevention or detection of serious crime.

[4] The confidence that information systems will protect the information they handle and will function as they need to when they need to, under the control of legitimate users.

Centre, which is responsible for facilitating the provision of interception (the content of communications) to all UK police and law enforcement agencies. Both SIS and GCHQ are regulated by the Intelligence Services Act 1994.[5]

2.4 The UK's intelligence analysis community is made up of a number of organisations with specific areas of expertise and organisational responsibility. The Chairman of the Joint Intelligence Committee (JIC) and Professional Head of Intelligence Analysis is responsible to the Prime Minister for supervising the work of the JIC. He is the head of the Joint Intelligence Organisation, which includes the Assessments Staff, a group of analysts responsible for drafting JIC papers and other products based on a range of sources that include reporting from the security and intelligence agencies, Defence Intelligence, the UK's diplomatic network and open source material.

2.5 Defence Intelligence (DI)[6] is a constituent part of the Ministry of Defence (MOD). It brings together expertise from all three Armed Forces as well as civilian staff. DI conducts intelligence analysis based on information from both overt and covert sources. It provides intelligence assessments in support of policy-making, crisis management and the generation of military capability. These are used by the MOD, military commands and deployed forces, as well as other Government Departments and to support the work of the JIC. In addition, DI is responsible for intelligence collection in support of defence and wider government requirements, for example: the Defence Geospatial Intelligence Fusion Centre provides the UK's specialist, advanced imagery intelligence to the armed forces and other intelligence partners through the exploitation of satellite imaging systems, in addition to airborne and ground-based collection systems.

2.6 The Joint Terrorism Analysis Centre (JTAC) is the UK's centre for all-source analysis and assessment of international terrorism. JTAC sets threat levels, and issues analytical reporting to Government Departments and agencies.

---

[5] S.3 of The Intelligence Services Act 1994 states: (1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be— (a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and (b) to provide advice and assistance about—(i) languages, including terminology used for technical matters, and (ii) cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.
(2) The functions referred to in subsection (1)(a) above shall be exercisable only—(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or (c) in support of the prevention or detection of serious crime.

[6] The UK's defence intelligence organisation, which is part of the Joint Forces Command, is the main provider of strategic intelligence to the Ministry of Defence and the Armed Forces. Defence Intelligence has four key roles: support to operations, support to contingency planning, provision of early warning of impending crises around the world and analysis of emerging threats. It provides collection capabilities, intelligence products and assessments to: guide decisions on policy and the commitment and employment of the Armed Forces; inform defence research and equipment programmes; and support military operations. It is also an essential element of the UK's central intelligence machinery, contributing staff and resources to the Cabinet Office in support of the Joint Intelligence Committee and to JTAC; and supports other government departments and NATO / EU military operations with advice and intelligence assessments.

Counter-terrorism operations

2.7 Since 2003, a comprehensive strategy has been in place to counter the threat to the UK and its interests overseas from terrorism. This strategy is known as CONTEST.[7] First published in 2006, it has since been revised and republished twice, in 2009 and 2011, to take account of the evolution of the threat and ongoing work to keep this country protected from harm. The CONTEST strategy covers all forms of terrorism and is based around four workstreams:

- ***Pursue:*** to stop terrorist attacks;
- ***Prevent:*** to stop people becoming terrorists or supporting terrorism;
- ***Protect:*** to strengthen our protection against a terrorist attack; and
- ***Prepare:*** to mitigate the impact of a terrorist attack.

2.8 Stopping terrorist attacks is the purpose of the *Pursue* strand of CONTEST. This means detecting and investigating threats at the earliest possible stage, disrupting terrorist activity before it can endanger the public and, wherever possible, prosecuting those responsible.

2.9 MI5 is responsible for the covert investigation of intelligence leads, calling on police resources from across the UK, including Police Scotland, as required. The UK's network of police counter-terrorism investigative and intelligence hubs and Special Branches contribute through the provision of local knowledge and specialist capabilities. Specifically this can include the development and management of Covert Human Intelligence Sources[8] (CHIS), Directed Surveillance,[9] or specialist financial investigation capabilities. Terrorist threats often have an overseas element,[10] and therefore MI5 in turn relies on the support of SIS and GCHQ to progress an investigation. As the terrorist threat has diversified in recent years,[11] the overseas elements of an investigation have become even more important.

---

7 *CONTEST: The United Kingdom Strategy for Countering Terrorism*, HM Government, July 2011, London, The Stationery Office.

8 Under the Regulation of Investigatory Powers Act 2000, a person is a covert human intelligence source (CHIS) if: a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c); b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. Home Office Code of Practice 2010.

9 Directed surveillance is covert surveillance in a public place that is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person.

10 Jonathan Evans, DG – Security Service, Address to the Worshipful Company of Security Professionals, 16 September 2010. https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-threat-to-national-security.html retrieved August 2013.

11 *CONTEST: The United Kingdom Strategy for Countering Terrorism*, HM Government, July 2011, London, The Stationery Office; and Annual Report on CONTEST: *The United Kingdom's Strategy for Countering Terrorism Annual Report*, HM Government, March 2013, London, The Stationery Office.

Box 2A: A typical example of how the security and intelligence agencies work together on an operation

An agent provides intelligence to MI5 suggesting that three men have travelled from the UK to an overseas terrorist training camp. MI5, SIS, and GCHQ set up a joint counter-terrorist operation.

MI5 directs the investigation into the three men, assesses the incoming intelligence and tasks further intelligence gathering. Each agency ensures that what they plan to do is necessary and proportionate, and has been properly authorised before capabilities are used. GCHQ seeks to derive intelligence from intercepting their communications overseas. SIS tasks its agents overseas with gathering intelligence on the men's intentions and plans. The police, Home Office and Foreign Office are kept informed.

An SIS agent is able to provide intelligence about the men's activities at the training camp and the date of their return to the UK. An MI5 surveillance team follows the men on their arrival in the UK.

MI5, SIS, and GCHQ continue to monitor the group, each Agency providing relevant intelligence streams. This identifies that they are in close contact with another subject of interest who is already being investigated under a different operation. Analysing various fragmented pieces of information allows the Agencies to discover details of a bomb plot. MI5 and the police work closely together as the MI5-led intelligence investigation moves towards police-led executive action.

After jointly reviewing the latest intelligence, MI5 and the police agree on the need to arrest the suspects. The police then make the arrests.

Forensic searches of the suspects' house generate further leads about terrorist activity, which are in turn investigated with intelligence input from the appropriate Agency.

2.10 The police service has lead responsibility (with the relevant prosecuting authority)[12] for the development of the evidential case and is responsible for all executive action resulting from counter-terrorism investigations in the UK.

2.11 Developments since 9/11, including the establishment of a regional MI5 presence, and the police counter-terrorism network throughout the UK, have meant that MI5–police relations – historically close have become even closer.[13] And it is the richness of their distinctive yet complementary skills brought together by the close working relationship between the security and intelligence agencies and the police which has been vital to the highly resilient and successful UK model for countering the terrorist threat for the benefit of the whole UK. The combination of devolved policing arrangements with powerful UK-wide and international security and intelligence agencies means Scotland enjoys the best of both worlds on matters of national security.

[12] Crown Office and Procurator Fiscal Service in Scotland, and the Crown Prosecution Service in England and Wales.

[13] Assistant Commissioner Bob Quick, testimony before the House of Commons Home Affairs Committee, Thursday 12 February 2009.

Box 2B: Operational and strategic co-ordination of counter-terrorism policing in the UK

Although the scope of the UK's counter-terrorism strategy (CONTEST) is UK-wide, policing is a devolved matter in Scotland and Northern Ireland, and there are differences as a result in governance, accountability, funding and legal arrangements between the Scottish and Northern Ireland police forces, and those in England and Wales.

Co-ordination structures have therefore been put in place by all UK chief constables working together so that their forces might support the aims of CONTEST most effectively and work actively as part of a UK police counter-terrorism network to help address the evolving threat by providing interoperable specialist counter-terrorism policing resources when required.

At governmental level, strategic oversight of the police counter-terrorism network is undertaken through the Police Counter-Terrorism Board, which includes senior police officers, including from Scotland, and which is chaired by a Home Office Minister. In support of this, oversight of counter-terrorism policing also forms part of the official-level CONTEST governance structures managed by the Office for Security and Counter-Terrorism (OSCT) at the Home Office. Scotland is represented in these structures just as OSCT representatives attend the Scotland CONTEST Board, which meets in Edinburgh.

2.12 It has been suggested that the Scottish Government has considered the Nordic intelligence services as a model for what an independent Scottish state might undertake.[14] In Denmark, Norway, Sweden and Finland, internal security is primarily a police lead. Military agencies also have a role in foreign and signals intelligence collection (for more information see Annex A). These latter roles are undertaken in the UK by SIS and GCHQ. The organisations and their responsibilities vary from country to country. Importantly, these capabilities were built up over a period of many years.

2.13 For this reason, establishing security and intelligence agencies on that model would not be without its challenges – both financial and human. Security and intelligence expert Baroness Ramsay of Cartvale states that "It should not be thought that a domestic security service of any standing or quality can be quickly developed from building on current Special Branch capabilities. It will take time, training and experience both to achieve the quality needed and also to demonstrate that quality to other services so that the advantages of exchanging expertise and information can be enjoyed".[15]

2.14 What is clear, given the global nature of terrorist and other threats (see paragraph 2.15 on espionage below), is that with access to the security and intelligence agencies, and the wider analytical community, of the UK, Police Scotland benefits from a considerable range of capabilities. These include information (e.g. intelligence reporting, raw data, records), technology (e.g. collection, processing, and analytic systems, databases, IT and communications infrastructure), processes (e.g. tradecraft, analytic techniques, security policies and procedures, information handling), people (e.g. Intelligence Officers and agents, analysts, linguists, systems engineers, cryptanalysts, IT experts) and

[14] Leask D, Scottish civil servants probe plans for 'Nordic' intelligence services after independence, http://www.heraldscotland.com/politics/referendum-news/scottish-civil-servants-probe-plans-for-nordic-intelligence-services-after-independence.21718032 retrieved 02 October 2013.

[15] Meta Ramsay – The Baroness Ramsay of Cartvale, Security service can take nothing for granted, Scotland on Sunday, 17 February 2013 http://www.scotsman.com/scotland-on-sunday-2-7506/opinion/comment/meta-ramsay-security-service-can-take-nothing-for-granted-1-2795918 retrieved 14 August 2013.

Partnerships (e.g. with international intelligence and security allies, the military, other government departments, industry partners and suppliers). An independent Scottish state would lose these capabilities and in the event of independence they would operate on behalf of the continuing UK.

2.15 These benefits are not limited to countering terrorism. The threat of espionage did not end with the collapse of Soviet communism in the early 1990s. Espionage against UK interests continues, is widespread, and potentially very damaging. In September 2010 the then Director General of MI5 warned that espionage presented a threat to the UK's commercial, diplomatic and defence interests.[16] The UK is a high priority espionage target. Many countries actively seek UK information and material to advance their own military, technological, political and economic programmes. Espionage activity is also increasingly carried out in cyberspace.[17]

2.16 While less visible to the public than the threat from terrorism, threats such as this continue to exist, as does the threat from the proliferation of weapons of mass destruction (WMD).[18] In certain, very significant respects such as cyber, these threats are growing (cyber is covered in more detail in chapter four). Dealing with these more traditional state related threats continues to be an important part of MI5's work and as a constituent part of the UK, Scotland along with the rest of the UK derives the benefits.

The security and intelligence agencies and international relationships

2.17 Key to the success of the security and intelligence agencies in combating terrorism and other global threats to the UK is the breadth and depth of their relationships with international partners. The UK is a member of the 'Counter Terrorism Group' which facilitates co-operation among European intelligence services. But these relationships are also global. British intelligence agencies are on record as working with over 200 partner services around the world.[19]

2.18 Of particular note among the UK's international relationships is the one it shares with Australia, Canada, New Zealand and the United States of America, also known as the 'Five-Eyes'. The relationship with the United States is close – a legacy of wartime co-operation sustained during the Cold War and since. It is through these relationships that the UK derives information which supports a wide range of policies, and it is able to do so because it makes a substantial contribution in return based on its own extensive capabilities. As a consequence of this intimate co-operation the UK derives a national security advantage that reaches far beyond the sharing of immediate threat related information and it benefits its security in a manner that would be severely affected if it were reduced in scale and capability.

2.19 There would be no automatic right of entry to the 'Five-Eyes' community for an independent Scottish state. The intelligence that these countries choose to collect and share is based on whether it is in their national interest to do so. Entry is by invitation only. No new country has been admitted for decades. There would have to be a benefit to the other members of an independent Scottish state joining – its unique contribution. An independent Scottish state may not posses the capabilities for this, and any new

[16] Jonathan Evans, Director General – Security Service, Address to the Worshipful Company of Security Professionals, 16 September 2010. www.mi5.gov.uk/home/news/news-by-category/speeches-and-statements/director-general-on-the-threats-to-national-security.html retrieved 25 October 2013.

[17] https://www.mi5.gov.uk/home/the-threats/espionage.html retrieved 27 July 2013.

[18] https://www.mi5.gov.uk/home/the-threats/proliferation-of-wmd.html retrieved 27 July 2013.

[19] Sir John Sawers, Chief of SIS, 'Britain's Secret Frontline', speech to the Society of Editors, 29 October 2010. See https://www.gov.uk/government/news/britains-secret-frontline-mi6-chief-speaks-in-public-for-the-first-time retrieved 14 August 2013.

capabilities would take time to mature.

Central intelligence machinery and the operation of the Control Principle

2.20 The UK's central intelligence machinery – the apparatus at the centre of Government, based in the Cabinet Office[20] – plays an important role between Ministers (the Prime Minister is accountable to Parliament for the Agencies collectively) and the operational work of the Agencies. Having developed and evolved its system for over a century, the UK draws the benefits from what is a sophisticated central intelligence apparatus.

2.21 An independent Scottish state would need to enact legislation to establish its own intelligence machinery; to provide strategic Ministerial oversight, accountability before Parliament, judicial oversight, and to regulate day-to-day operations. Assessments Staff and a broader all-source analytical capability would also need to be recruited and trained, and a system established to determine the requirements and priorities for intelligence collection. Such a mechanism would be essential.

2.22 In establishing its own intelligence machinery, and in anticipation of working with overseas partners, an independent Scottish state would have to put in place its own government security policy and establish systems to secure Scottish secrets. It would also have to address the issue of the 'Control Principle'. This dictates that the service who first obtains the intelligence has the right to control how it is used; who else it can be shared with, and what action can be taken on it.[21]

Box 2C: Operation of the 'Control Principle'

"This rule [also] known as the Third-Party Rule, is of fundamental importance in the intelligence community, and the consequences of breaking it are – at best – a drying up of that source of information, if not a wider breakdown in relations between the two parties".[1]

[1] Grant G, *In Scotland's Defence? An Assessment of SNP Defence Strategy*, Henry Jackson Society. July 2013.

2.23 The UK could not share secret intelligence with an independent Scottish state that had been passed to it by a third country, such as the US, without the third country's consent. No other nation shares secret intelligence without assurances on their material being properly protected by physical and personnel security measures as well as a legal framework that allows for the (Control Principle) to operate. The adoption of the relevant policies and practices would not by themselves be enough to facilitate intelligence sharing. It is also a matter of trust and confidence, which would take time to build up – not only with the continuing UK but with other intelligence agencies around the world. There would be no immediate intelligence dividend.

2.24 An independent Scottish state would need to develop its own security and intelligence agencies. It could not 'share' the UK's security and intelligence agencies for reasons of sovereignty and democratic accountability, as well the critical role they play in the UK's defence and foreign policies. In addition, as the first Scotland analysis paper in the series, *Devolution and the implications of Scottish independence* made clear, all of the current powers and responsibilities of the UK in Scotland would become the responsibility of a new independent Scottish state; and this would include security, defence and

[20] *National Intelligence Machinery Booklet*, Cabinet Office, November 2010, page 19.
[21] Sir John Sawers, Chief of SIS, 'Britain's Secret Frontline', speech to the Society of Editors, 29 October 2010.

intelligence. The security and intelligence agencies would therefore continue to operate in the national interest of the continuing UK and in accordance with the priorities set for them by the UK Government. Responsibility for their activities would continue to lie with UK Ministers who are, and would continue to remain, accountable to Parliament at Westminster.

The costs of establishing a security and intelligence capability

2.25 The sixth paper in the Scotland analysis series on defence made clear that various proposals or options have been put forward by the Scottish National Party (SNP) and others regarding the possible defence posture and capabilities of an independent Scottish state, with estimated costs ranging from £1.6 billion to £2.5 billion to cover defence, intelligence and cyber capabilities. Even the highest of these estimates (the SNP's proposal) is only about 7 per cent of the combined UK budgets for defence, intelligence and cyber, and less than countries such as Denmark and Norway spend on defence alone.

2.26 In her evidence to the Foreign Affairs Committee's inquiry into the foreign policy aspects of Scottish independence,[22] the Deputy First Minister was asked about the set up costs of developing separate intelligence and cyber security capabilities, given that the UK had devoted billions of pounds to developing its infrastructure over several decades. The Deputy First Minister did not provide an answer but did refer the Committee to the ongoing work being undertaken by the Scottish Government towards publishing a White Paper.

2.27 It is unclear what level of security and protection the Scottish Government's proposals would provide for an independent Scottish state. Nor is it clear what additional funding the Scottish Government will set aside for these initial set up costs. Nor has it been explained what trade-offs will be made against other priorities such as health and pensions to pay for this, assuming that the proposed £2.5 billion budget for defence and security is for running costs only.

Interception and communications data

2.28 The UK benefits from a system, established under the Regulation of Investigatory Powers Act 2000, that enables the interception of communications and the acquisition of communications data for lawful purposes. These capabilities make an enormous contribution to the prevention and detection of crime throughout the UK. They are also central to the investigation and disruption of terrorist plots. The use of these techniques can be intrusive. They are therefore governed by a stringent set of safeguards, which are kept under constant review.

2.29 Interception (such as the monitoring of phone calls or emails) is in particular subject to a robust array of checks and balances. The ability to undertake interception is limited to a small number of bodies, defined in legislation, and for a limited range of purposes (national security, preventing and detecting serious crime, and safeguarding the economic well-being of the UK). Interception must be authorised by the relevant Secretary of State. The use of communications data (subscriber information or information *about* a call or correspondence) is less intrusive and can be used by the police and other specified public authorities when authorised as necessary and proportionate for specific purposes set out in statute. Communications data is a crucial

[22] House of Commons Foreign Affairs Select Committee – Sixth Report – Foreign policy considerations for the UK and Scotland in the event of Scotland becoming an independent country (1 May 2013). HC 643, London, The Stationery Office. http://www.publications.parliament.uk/pa/cm201213/cmselect/cmfaff/643/64302.htm retrieved August 2013.

tool for the police in the investigation and prosecution of a wide range of crimes, and also in other areas of public safety.

2.30 In line with the EU Data Retention Directive, the UK places legal obligations on Communications Service Providers (CSPs) to ensure that they retain specific types of communications data under Data Retention Regulations. This ensures that relevant data will be available if required by public authorities where necessary and proportionate for specified investigatory purposes. The Government can also place requirements on CSPs to provide interception capabilities in order to give effect to warrants served upon them.

Conclusion

2.31 As a part of the UK, Scotland benefits from a range of skills, capabilities, mature and well resourced security and intelligence agencies, as well as established national infrastructure that deliver security benefits to the whole of the UK. An independent Scottish state would have to make separate provision for the protection of its national security.

Chapter 3: Justice, policing, and combating serious and organised crime

- Long established UK-wide laws facilitate the cross-border pursuit of justice by enabling straightforward judicial and police co-operation despite different legal systems and police jurisdictions across the UK.
- A search warrant issued by a court in Scotland can be executed in the rest of the UK (and vice versa) with the minimum of bureaucracy. This ensures that evidence can be gathered from different legal jurisdictions in the UK more quickly and efficiently than is possible, for example, between EU Member States.
- Officers from Police Scotland have the powers to arrest and detain suspects in the rest of the UK (and vice versa). This facilitates both the day-to-day pursuit of justice across the UK and also provides the essential foundation for police mutual-aid in emergencies such as civil disorder or terrorism. This would lapse with the establishment of an independent Scottish state because the laws and institutions that underpin them would cease to exist.
- Even in the EU, where some countries permit cross-border hot pursuit, these arrangements do not replace the need for European Arrest Warrants in any circumstances.
- Organised criminals do not respect borders – including between Scotland and the rest of the UK – but rather work to exploit them, capitalising on the additional challenges faced by law enforcement agencies when responding to cross border crime. Organised criminals may seek to exploit a new international border, perceiving a more exposed target or potential legal loopholes.
- UK-wide agencies have crucial roles to play – often holding relevant information and powers which can disrupt Organised Crime Groups impacting on Scotland.
- At present Police Scotland has automatic access to national police databases and the National Crime Agency (NCA) providing intelligence reporting to Police Scotland and vice versa. An independent Scottish state would lose guaranteed access to the wider information and intelligence picture provided by national police structures and the NCA.
- The UK's national and international links are critical to it effectively managing the threat. Scotland would lose direct access to the NCA's international network and to its specialist and niche capabilities.

- The benefits of the close working relationship between Scotland and the rest of the UK in tackling cross-border and organised crime are clear. With devolved policing and its own organised crime strategy, supported and enhanced by the resources and capabilities of the NCA, Scotland's fight against serious and organised crime is strengthened by its membership of the UK.

Judicial and police co-operation

3.1 The UK has three separate legal systems, in England and Wales, Scotland and Northern Ireland. The UK Supreme Court is the final court of appeal for all UK civil cases, and criminal cases from England, Wales and Northern Ireland. The High Court of Justiciary, sitting as an Appeal Court, is the final court of appeal in Scottish criminal cases and its decisions, subject to certain limited exceptions,[1] are not subject to review.

3.2 Parliament recognised as long ago as the nineteenth century that, to facilitate the effective rendering of mutual legal assistance between these jurisdictions, legal authorities from any part of the UK should be able to cooperate as much as possible, and with the minimum of formality, in the investigation and detection of crime. It was for that purpose that it enacted legislation which continues to this day to facilitate this.[2]

Box 3A: Cross border search warrants

Legislation ensures that a search warrant issued by a court in Scotland and endorsed by a court in England can be executed as would a warrant issued by the endorsing court and by an officer of either court. This means that in the pursuit of justice, while the UK's different legal systems may be distinct, they are entirely capable of working directly with each other.

3.3 The benefit of the process highlighted in Box 3A is that the endorsing judge is only required to verify the signature of the issuing judge. This is in contrast to the system operating between the UK and other countries (including EU Member States) where the request for a search warrant (or a production order) must be considered by the Secretary of State or Lord Advocate (in practice 'central authorities' acting on their behalf) who then direct an officer to make an application to the court for a search warrant in line with domestic requirements (and also subject to dual criminality).[3,4] In contrast, the UK's own internal legislation has stood the test of time and challenge as recently as 1999 in R v Manchester Stipendiary Magistrate etc.

---

1 The main exception is that in certain circumstances the Supreme Court may consider 'devolution issues' arising in Scottish criminal cases. Some of these devolution issues are now called 'compatibility issues' due to changes made by the Scotland Act 2012; cases which involve human rights or EU law points. Devolution issues cover other matters about devolved competence of the Scottish Ministers or legislative competence of the Scottish Parliament. In certain circumstances it is also possible to take a human rights point in a Scottish criminal case to the European Court of Human Rights in Strasbourg.

2 S.4 Summary Jurisdiction (Process) Act 1881, and S.29 Petty Sessions (Ireland) Act 1851. Also see House of Lords, *Regina* v. Manchester Stipendiary Magistrate and the Lord Advocate (Appellants) Ex Parte Granada Television Ltd. (Respondent), 14 December 1999. http://www.publications.parliament.uk/pa/ld199900/ldjudgmt/jd991214/granad-1.htm retrieved August 2013.

3 'Dual criminality' means that for someone to be extradited, their alleged conduct has to be a criminal offence in both the surrendering and the requesting state.

4 S.16-19 Crime (International Co-operation) Act 2003, http://www.legislation.gov.uk/ukpga/2003/32/contents retrieved August 2013.

Box 3B: Operation of the European Arrest Warrant

93 days was the average length of time it took to extradite somebody from the UK using the European Arrest Warrant in 2010 where the person did not consent to the surrender. It was 16 days where the person agreed to the surrender.[1]

In contrast, the arrest and return of offenders between England or Wales and Scotland and Northern Ireland is usually dealt with on a cross-border enforcement basis.

This means that a domestic warrant issued in one jurisdiction may be executed without any endorsement or judicial intervention in the other jurisdiction. There are corresponding cross-border powers of arrest by constables from one jurisdiction in another.[2]

[1] Replies to questionnaire on quantitative information on the practical operation of the European arrest warrant – Year 2010, Council of the European Union document 9120/2/11 REV 2, 9 September 2011. http://register.consilium.europa.eu/pdf/en/11/st09/st09120-re02.en11.pdf retrieved 02 August 2013

[2] Cross-border enforcement, CPS website, http://www.cps.gov.uk/legal/v_to_z/withdrawal_of_bench_warrants/ retrieved 02 August 2013.

3.4 Mutually beneficial co-operation between criminal justice systems in the UK is not limited to the role of the courts. The scope for law enforcement co-operation in the pursuit of suspects and fugitives from justice is considerable. The Criminal Justice and Public Order Act 1994 makes extensive provision for cross-border powers of arrest and detention. The benefits of this are not limited to cross-border arrests.

3.5 The UK policing model offers enormous scope and capability to render mutual aid in responding to one-off events which threaten to overwhelm any individual force. This includes responding to terrorism-related threats, as well as civil disorder. Mutual aid arrangements during the 2005 G8 Summit in Gleneagles saw police forces from across the UK providing support to their counterparts in Scotland. The 2011 riots in England saw non-English forces, including from Scotland, lending support to their counterparts in the England. Police forces from the rest of the UK were involved in providing support during the 2012 Olympic Games[5] and they stand ready to do so again during the 2014 Commonwealth Games.

3.6 The creation of an independent Scottish state would mean the cessation of police mutual aid arrangements as presently understood because of the loss of existing arrest and detention powers for officers operating across what would become the continuing UK – Scotland border. This is because the applicable legislation – enacted by the UK's Parliament, and overseen by the UK's Supreme Court – would cease to apply. This in turn risks upsetting a vital cross-border capability, which would have implications for emergency service planning in both countries. The creation of an independent Scottish state also risks impacting on how the two states deal with serious and organised crime.

[5] Mutual Aid Resources for London 2012 Olympic and Paralympic Games, Metropolitan Police Media Library. Retrieved 23 August 2012, http://media.met.police.uk/documents/MutualAid.pdf

Box 3C: Cross border hot pursuit in the EU

Under the EU's Schengen policing and justice arrangements, some EU countries permit the police from neighbouring states to undertake cross-border hot pursuit operations. However, these do not allow them to arrest suspects in another Member State, or bring them back across the border. The most the pursuing officers can do is detain the suspect until the local police can arrive on the scene and make an arrest.

These arrangements therefore do not replace the need for European Arrest Warrants in any circumstances. Furthermore, the UK is not party to these arrangements. As regards the UK's land border with the Republic of Ireland, officers of the Police Service of Northern Ireland and An Garda Síochána have no powers of arrest in each other jurisdiction, and there are no powers of cross-border hot pursuit operating across the border.

Box 3D: Drug baron fought extradition from Ireland for two years before being jailed in the UK for 18 years[1]

An international drug dealer who was extradited from Ireland to face charges he imported millions of pounds worth of cocaine and cannabis into the UK was jailed for 18 years.

Philip Baron, a former HGV driver from Salford, was the kingpin in an international ring who owned yachts and sports cars as well as luxury villas in Spain, all funded by drug money. Baron, who was living near five-star golf resort the K Club in Ireland, had fought extradition to the UK for two years. He was extradited to the UK in November 2012.

He admitted three counts at Liverpool Crown Court, including conspiracy to import cocaine between March and November 2008, conspiracy to import cannabis between September 2005 and September 2009, and money laundering.

An officer from the Serious Organised Crime Agency, who can only be identified as Mark, said: "The evidence that we have has shown that they have literally hammered the UK's streets with drugs. Over a prolonged period they lived with impunity from aboard and controlled that organisation from aboard while living luxurious lifestyles. These guys were absolutely prolific."[2]

---

1 According to Dr Gavin Barrett, under the European Arrest Warrant system in Ireland, on average, 50 per cent of individuals do not contest their surrender and in those cases a surrender can be effected in between six and seven weeks. Where a case is contested it will take about five to nine months to effect a surrender and to go through the process of surrender. 'There have been very rare cases that have gone a long way through the courts and gone on for a period of years. It is extremely rare, although not unheard of, it has to be said, for an appeal against surrender to be successful." Evidence to the House of Lords EU Committee on the UK's 2014 Opt-Out Decision, 13 February 2013, http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/Protocol36OptOut/VolofevidenceP36asat250313.pdf retrieved 11 September 2013.

2 Hall, M. English 'gentleman' who funded champagne lifestyle with £300m in drugs money, The Daily Telegraph, 26 March 2013. http://www.telegraph.co.uk/news/uknews/crime/9956247/English-gentleman-who-funded-champagne-lifestyle-with-300m-in-drugs-money.html; and, Drug baron extradited from Ireland jailed in UK, The Irish Times, 20 June 2013. http://www.irishtimes.com/news/world/uk/drug-baron-extradited-from-ireland-jailed-in-uk-1.1436655 retrieved 11 September 2013.

Serious and organised crime

3.7 The National Security Strategy highlights organised crime as a tier two risk to national security (related risks under the NSS are border security, a tier three national security risk, and cyber, a tier one risk that encompasses large scale cyber crime). Its impacts are increasingly recognised alongside more traditionally understood threats, while at the same time it is the case that, unlike terrorism, organised crime consists of a cumulative series of events rather than a cataclysmic one-off event.[6]

3.8 Organised crime is a multi-billion pound enterprise. According to the UK Government's Serious and Organised Crime Strategy it costs the UK at least £24 billion each year. The Scottish Government estimates that the social and economic costs of drugs misuse in Scotland are £2.6 billion per year and the cost of fraud, much of which is perpetuated by Organised Crime Groups (OCGs), costs each person in Scotland £330 each year.[7]

3.9 Everyone is affected by organised crime. It fuels street crime and increases fear through violence and intimidation. It brings misery to thousands of families through drug peddling. It undermines legitimate hard-working businesses, which costs Scotland's economy in jobs and wealth creation. Over 350 OCGs comprising more than 4,000 individuals are believed to be operating in Scotland.[8] Published estimates from 2009 indicated that 92 per cent of OCGs in Scotland were involved in drug related crime and more than half of OCGs were involved in a range of crime types. The top 20 groups (in terms of highest threat) were operating across all of Scotland's then police force areas (before the establishment of Police Scotland).[9] Many of these groups and individuals will have international links.

3.10 OCGs recognise neither organisational boundaries nor national and international borders, but rather work to exploit them, capitalising on the additional challenges faced by law enforcement agencies when tackling a cross border threat. OCGs would thus operate on both sides of the continuing UK-Scotland border, with its existence having little or no impact on their criminal enterprise. For example, there are well known links between Merseyside-based organised criminals and criminal activity in Scotland.[10] Likewise, OCGs operate across borders between England, Northern Ireland and Wales.

3.11 There is therefore a need for law enforcement and other agencies to work collaboratively across force and institutional boundaries where the threat is such that the operational response requires more cross-cutting coordination, as is the case with organised crime. Therefore, whilst policing is devolved to Scotland, on matters of cross-border crime threats Police Scotland has quick and easy access to the intelligence, resources and expertise of police forces in England and Wales and the NCA to help tackle the threats where needed. The flexibility and responsiveness of this operational relationship works

---

6 *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government, 2010, London, The Stationery Office.

7 http://www.scotland.gov.uk/Topics/Justice/crimes/organised-crime retrieved 16 August 2013.

8 *One Year On, Letting Our Communities Flourish: A Strategy for Tackling Serious Organised Crime in Scotland*. The Scottish Government 2010, Edinburgh, http://www.scotland.gov.uk/Resource/Doc/313639/0099447.pdf retrieved 14 October 2013.

9 Preliminary findings on the scale and extent of serious organised crime in Scotland: Scottish serious organised crime group mapping project, http://scotland.gov.uk/Resource/Doc/254429/0098144.pdf retrieved 02 September 2013.

10 See for example http://www.clickliverpool.com/news/national-news/1211789-liverpool-organised-crime-gang-jailed-for-drugs-and-firearms-conspiracy-.html; or http://www.heraldscotland.com/mobile/news/home-news/gangster-and-his-daughter-jailed-after-drug-gang-foiled.18406574?_=3ffe509517936b27abdb5cb74f219bbbf5c7e221 retrieved 30 August 2013.

both ways with police forces in England and Wales police forces and the NCA drawing on the intelligence and resources of Police Scotland. This mutually beneficial operational relationship, which respects the devolution of policing, allows for a dynamic collective operational response to serious and organised crime threats where no one police force or agency is left without the access to the expertise and resources that may need to be drawn on from across law enforcement.

3.12 The growing sophistication of organised criminals means that activities to disrupt them are also likely to become more complex, requiring greater innovation, international co-operation and technical skills. The collective UK law enforcement response needs to be as flexible and nimble as the OCGs it tackles, but the jurisdictional and practical barriers to co-operation that would result if an independent Scottish state was established would reduce the effectiveness of efforts to investigate, prosecute and convict these criminals by all parties. Organised criminals may seek to exploit an independent Scottish state and the UK sharing a common border, perceiving a more vulnerable target or potential legal loopholes.

Box 3D: Operation Laurel

A joint operation by Merseyside and Scottish police uncovered a major drug-trafficking ring being run from a prisoner's cell.

Paul McIntyre, from Liverpool, ran the ring while serving a 45-month sentence for drug dealing at Saughton prison in Edinburgh. He used mobile phones to co-ordinate a supply chain that ran from his native Liverpool, where he was connected to a gang known as the Baker's Green Boys, to Saughton prison and HMP Addiewell in West Lothian.

Police in Edinburgh and Merseyside put his four-man team of drug dealers under surveillance and swooped after watching them carry out three major drugs transactions while McIntyre was behind bars. McIntyre was sentenced to a further nine years and six months for being concerned in the supply of heroin and cocaine at HMP Saughton and HMP Addiewell, as well as on the Edinburgh City Bypass and the A74 (M) at Ecclefechan, Dumfries and Galloway. The police intercepted 6.18 kilograms of heroin with a street value of £611,900 and 2.55 kilos of cocaine valued at £101,640.

3.13 In 2009 the publication of 'Letting our Communities Flourish' set out Scotland's strategy for combating serious organised crime. The strategy was drafted in partnership with members of the Serious Organised Crime Taskforce, including UK-wide agencies.[11] The creation of Police Scotland (which merged the Scottish police forces and the Scottish Crime and Drugs Enforcement Agency) and the structures within it to tackle serious and organised crime through the Specialist Crime Division[12] show that Scotland has a well developed infrastructure to tackle organised crime. However, the UK's national and international links and collective capabilities are also fundamental to it effectively managing the threat. Indeed, Scotland's Serious Organised Crime Strategy explicitly acknowledges that UK bodies such as the Serious Organised Crime Agency (SOCA, now replaced by the National Crime Agency), HM Revenue and Customs, the Department for Work and Pensions and the Health and Safety Executive have crucial roles to play, often holding relevant information or enforcement powers which can help

[11] http://www.scotland.gov.uk/Topics/Justice/crimes/organised-crime/soc/strategy Retrieved 22 October 2013.

[12] The Specialist Crime Division (SCD) provides specialist investigative and intelligence functions such as Major Crime investigation, Public Protection, Organised Crime, Counter Terrorism, Intelligence and Safer Communities. See www.scotland.police.uk retrieved 11 October 2013.

disrupt organised crime groups.[13] The NCA also presents an outstanding opportunity to achieve a further step-change in the UK's response, not just against organised crime, but also against other forms of serious crime that require a co-ordinated national operational response. It will deliver a more integrated response, including with Police Scotland, which will further benefit the whole of the UK.

3.14 The NCA will build on SOCA's experience and partnerships working with Police Scotland. Whilst the NCA is a UK-wide agency, it was created with the consent of the Scottish Parliament and its activities in Scotland are governed by specific statutory arrangements to reflect the devolution of policing. The Scottish Government and Police Scotland were engaged with and consulted on critical decision-making at the UK level in the creation of this new national agency to ensure that its design and response would work as effectively in Scotland as across the whole of the UK. From early next year, the co-location of the NCA in Scotland at the Scottish Crime Campus at Gartcosh[14] with Police Scotland and wider law-enforcement partners will further enhance the strong operational relationships that benefit the collective operational response to serious and organised crime.

3.15 This strategic level input works both ways and is complemented by the NCA's membership of the Scottish Serious Organised Crime Taskforce (SOCTF). The NCA's presence at this key policy-setting forum ensures that its activities in Scotland remain consistent with Scotland's wider strategic priorities in relation to serious organised crime. The NCA participates in the Scottish national tasking regime, chaired by Police Scotland, and has officers embedded at the Crown Office and Procurator Fiscal Service and within the multi-agency unit housed within the Police Scotland National Intelligence Bureau. In turn, Police Scotland attends the National Strategic Tasking and Co-ordination Group and the National Tactical Tasking and Co-ordination Group meetings chaired by the NCA.

[13] *Letting Our Communities Flourish: A Strategy for Tackling Serious Organised Crime in Scotland*, The Scottish Government, 2009, Edinburgh, RR Donnelley.

[14] Details of the Scottish Crime Campus at Gartcosh can be found at http://www.scotland.gov.uk/Topics/Justice/crimes/organised-crime retrieved 11 October 2013

Box 3E: Operation Knot

Operation Knot was a long running operation managed in partnership between Scottish Law Enforcement and the North West England Regional Organised Crime Unit (Titan). It centred on a cross-border organised crime group concerned in the importation and distribution of Class A Drugs.

Joint working smashed the drug cartel and put 13 people – including a father and daughter – behind bars for 152 years. Gang leaders John Cooke, 32, of Birkdale, Merseyside, and James Swarez, 44, of Crosby, Merseyside, were both jailed for 17 years at Liverpool Crown Court after pleading guilty to conspiracy to supply controlled drugs.

The pair, described by police as "major players" in the drugs trade by the police, obtained high purity drugs from trafficker Paul McDonald, 44, and used a network of couriers in Glasgow, Cardiff, Preston and Ellesmere Port.

Merseyside-based McDonald also admitted conspiracy to supply controlled drugs and was jailed for 15 years. Ten other gang members, who were used as couriers, received jail sentences of between five and 12 years. Among the drug couriers were Edward McCreadie and his daughter Roseanne, both of Rutherglen, South Lanarkshire, and Gordon Smith, 49, of Glasgow.

Edward McCreadie ran the Scottish arm of the "national enterprise" with the help of his daughter, and teamed up with Liverpool crime bosses to handle shipments from England. He pleaded guilty to dealing at Liverpool Crown Court and a sentence of 12 years and eight months was handed down. Roseanne McCreadie was jailed for nine years.

Class A drugs with a street value of more than £1 million were seized.

3.16 The NCA, which launched on 7 October 2013, leads the UK's fight to cut serious and organised crime, with improved sharing of enforcement and intelligence resources facilitating a wider ranging and more effective law enforcement approach to combating serious and organised crime. The NCA provides a range of enhanced national capabilities and specialist/niche capabilities to support and benefit law enforcement partners – including Scotland.

3.17 Examples of NCA capabilities which have a UK-wide national reach, and that have been used to support the efforts of Police Scotland, are provided below (and in greater detail in Annex B). In a number of cases, Police Scotland has in-house capabilities and only calls upon the NCA when additional resources are needed on a surge basis or where additional specialist or sensitive expertise is needed. In other cases, the capabilities within the NCA are provided on a UK-wide basis and are not replicated elsewhere. An independent Scottish state would have to consider whether to further invest in or replicate these capabilities.

- Child Exploitation and Online Protection Command
- UK Human Trafficking Centre
- UK Financial Intelligence Unit
- UK National Central Office for Counterfeit Currency
- Missing Persons Bureau
- Anti-Kidnap and Extortion Unit
- Serious Crime Analysis Centre

- Specialist Operations Centre
- Crime Operational Support
- Illicit Laboratory Team
- International liaison network
- Interpol / Europol liaison
- Specialist cyber support
- Technical collection
- Technical Operations Support
- Specialist surveillance

3.18 In the event of a vote for independence, Scotland would need to determine which of those NCA and other lead-force capabilities it would want to replicate and how it would be provided for.

NCA Intelligence Hub

3.19 The NCA Intelligence Hub is responsible for informing the response to criminal threats based on a single, authoritative, intelligence picture and will routinely shares intelligence assessed reporting with Police Scotland. The NCA Intelligence Hub is able to access and fuse different sources of intelligence to add value that other parts of law enforcement cannot, and to assess the impact of activities against serious and organised crime. The NCA is able to receive and pass information to UK police forces, UK law enforcement agencies and other organisations, both in the UK and abroad. The Crime and Courts Act places a duty on the NCA to keep all UK police forces, including Police Scotland, informed of relevant information.

3.20 In the event of a vote for independence the relationship with the Intelligence Hub would change. While in the interests of crime prevention there would still be an intelligence sharing relationship, overall it is likely that this would be modelled on data sharing arrangements with other European law enforcement partners rather than governed by local domestic arrangements. At the very least it is expected that the continuing UK-Scotland intelligence sharing relationship would need to be renegotiated. This could be to the detriment of law enforcement on both sides of the border but would be a natural outcome of separate polities with differing levels of engagement and intelligence sharing with other international partners.

Niche and specialist capabilities

3.21 Beyond the NCA there are also police capabilities managed by one police force or region that benefit all of the UK. An independent Scottish state would need to decide which, if any, of these capabilities or networks it would want to replicate or keep. For example, the National Fraud Intelligence Bureau is managed by the City of London Police, but operates across the UK. This national infrastructure benefits all of the UK by providing centres of expertise and economies of scale and the establishment of an independent Scottish state would be likely to result in increased costs for all parties.

3.22 The international dimension to the response to serious and organised crime is vital. Organised crime causes, and is fed by, instability that in turn threatens the UK, and efforts to tackle it must include work to promote effective criminal justice systems in source and transit countries, and promote the rule of law. The scale and range of UK overseas effort to reduce the organised crime threat to the UK and its interests is commensurate with the UK's economic strength and is key to the ability to tackle upstream activity impacting upon the UK, such as drug trafficking, organised immigration crime, fraud and cyber crime.

3.23 The NCA has an international network of around 120 officers based in around 40 countries. Its international presence acts as a "force multiplier", enabling it to leverage the efforts of partners in the UK's interests and address the problem of organised crime before it reaches the UK, which is more cost effective. The network represents both the NCA and the wider UK law enforcement community, and collaborates with overseas partners at different levels and in diverse forums. In the event of a vote for an independent Scotland, it would be a matter for an independent Scottish state to decide whether to invest in creating a similar network of Scottish officers.

3.24 While an independent Scottish state would be likely to continue to benefit indirectly from the efforts of the network, it would not be able to target and influence relationships to concentrate on issues of particular significance to Scotland. Several of the UK's national agencies working to reduce the organised crime threat to the UK and its interests deploy officers overseas to tackle threats at source and en route to the UK. While the largest of these is the NCA's network of liaison officers, Her Majesty's Revenue and Customs (HMRC) also has a network of around 25 Fiscal Crime Liaison Officers (FCLOs) who tackle the full range of fiscal crime issues, including fiscal fraud committed by organised criminals, such as tobacco smuggling.

3.25 The Home Office also has its Risk and Liaison Overseas Network of around 90 officers working on a range of immigration liaison matters, including organised immigration crime. In addition to this, the Crown Prosecution Service also has a small network of Criminal Justice Advisors and liaison magistrates working in key threat countries to improve the Rule of Law and help those countries act more effectively against serious and organised criminals operating from or present there. While Scotland's prosecutorial service (the Crown Office and Procurator Fiscal Service) is separate to the Crown Prosecution Service, this work to advance a more effective and fair legal and judicial system in key threat countries benefits all parts of the UK. While an independent Scottish state is likely to be able to continue to benefit from this work, what it would lose is the ability to influence the deployment and activities of these advisors.

International partnerships

3.26 The UK and UK agencies such as the NCA benefit from strategic relationships with a range of international partners including governments and law enforcement agencies which are often based on or enabled via memoranda of understanding (MOU). These would need to be renegotiated, and in many cases this may risk a less favourable outcome for both Scotland and the continuing UK.

3.27 Significantly, the UK enjoys a strategic partnership with the US on organised crime. The strategic partnership drives co-operation across a broad range of activity and leverages the weight of skills and resources available to both nations from research partnership, through intelligence gathering and sharing, to operational partnership and international leadership on issues such as the links between organised crime and terrorism. There are significant advantages for Scotland in such UK wide partnerships.

3.28 Furthermore the UK has significant influence in multilateral fora such as the Council of Europe, the G6 and G8, the UNODC and the Financial Action Taskforce. Its achievements in these fora help reduce the organised crime threat to the UK, and its influence allows it to achieve more by working in partnership on strategic issues such as establishing and driving international standards in the fight against cyber crime or money laundering and terrorist financing. Membership of these groups will not be an automatic right for an independent Scotland.

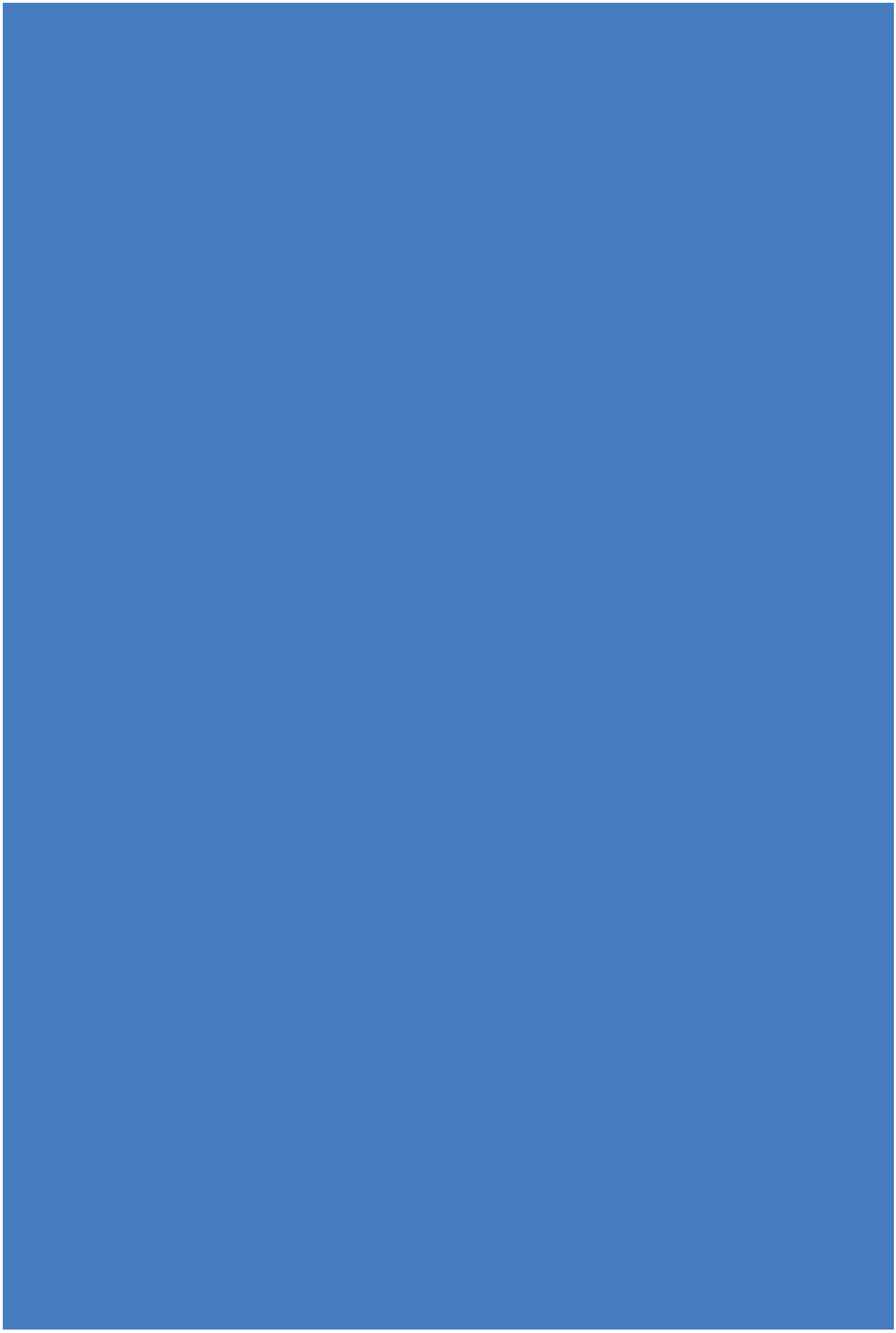
3.29 The NCA works in collaboration with international law enforcement partners from Australia, Canada, New Zealand and the USA as part of the Strategic Alliance Group (SAG). The Group seeks to reduce the international threat and impact of organised crime.[15] With common threats and ever greater pressure on resources, sharing intelligence and committing shared resources to tackling these threats is the key focus of the group.

3.30 Beyond the practicalities of co-operation, intelligence sharing and shared resources, the UK also currently benefits from legislative alignments, for example the Misuse of Drugs Act 1971. Although there are some differences in the secondary legislation made under the 1971 Act, the Act provides a robust framework for the UK through appropriate controls based on the ABC classification system. A uniform UK-wide control framework benefits both Scotland and the rest of the UK and prevents criminals residing in one country while committing offences in another due to differences in penalties for specific offences.

Conclusion

3.31 The benefits of the current close working relationship between Scotland and the rest of the UK in tackling organised crime are clear. Long standing judicial and policing co-operation, and mature collaborative arrangements across a number of agencies, enables a coherent picture of the threat and for a prioritised approach to tackling organised criminal groups to be taken. An independent Scottish state could not rely on the status quo and would be likely to have to renegotiate relationships and provide significant additional resource in order to enjoy the benefits that it currently gains as a constituent part of the UK. From financing international liaison to passing new legislation to meet international obligations, it would be a significant burden for a new state to take on.

[15] Eight agencies are represented on the group: Australian Crime Commission, Australian Federal Police, US Drug Enforcement Administration, US Federal Bureau of Investigation, US Immigration and Customs Enforcement, New Zealand Police, Royal Canadian Mounted Police, and the Serious Organised Crime Agency.



Chapter 4:
Cyber and protective security, and resilience

- Cyber security threats come from a range of actors including criminals, states, terrorists, and hacktivists. According to PwC the average cost to a small business in the UK of their worst security breach of the year is £35,000 - £65,000. This is £450,000 - £850,000 for large organisations.
- As a part of the UK, Scotland benefits from an £860 million five year National Cyber Security Programme which has already delivered a number of benefits including the shutting down of over 1,000 fraudulent websites by HMRC, and the introduction of systems which enable the public to report cyber-enabled crime – facilitating a joined-up UK-wide approach.
- Successfully delivering cyber security adds to the overall competitiveness of the UK which benefits businesses across the country, including those in Scotland, and makes the UK an attractive place to invest.
- Delivering a successful cyber security programme in the UK requires the recruitment and retention of highly skilled and scarce cyber security experts in competition with the private sector, as well as considerable financial investment.
- An independent Scottish state would require new investment in basic cyber security infrastructure – funded from within defence and security budget.
- The UK has well established arrangements in place for the protection of Government assets, including information and people. As set out in the first paper in the Scotland analysis series *Devolution and the implications of Scottish independence,* an independent Scottish state would not be party to the UK's existing international agreements. This would include the applicable international security agreements that facilitate the flow of classified information with international organisations like NATO and the EU.
- Terrorists continue to aspire to obtain chemical, biological, radiological and nuclear (CBRN) devices. The UK Government maintains a number of national capabilities to deal with such devices as well as explosive materials.
- The UK also maintains a decontamination service to clean up after any CBRN incident. Access to international mutual aid for civil protection will be an important aspect of any negotiations on membership by an independent Scottish state in joining the EU and NATO.

- The UK operates a scheme to prevent specified foreign national passengers who pose a terrorist threat from travelling to the UK, and to prevent British nationals boarding flights when assessed to pose a direct threat to the aircraft. An independent Scottish state would have to make its own arrangements.
- Scotland benefits from the best of both worlds: devolution within the UK, underpinned by the unconditional availability of protective assets and capabilities funded and delivered on a UK-wide basis. This ensures that every citizen and every part of the UK is better protected.

Cyber security

4.1 The internet has revolutionised modern society, driving economic growth and giving people new ways to connect and co-operate with one another. It does not, however, come without its risks.

4.2 These risks come from several actors – criminals – cyber means can give 'offline' illegal activity unparalleled scale and reach; states – engaged in espionage, or the compromising of our government, military, industrial or economic assets; terrorists – who seek to radicalise potential supporters, spread propaganda, communicate and plan attacks; and politically motivated hacktivists who may be interested in attacking public and private sector websites and online services.

4.3 According to PwC the average cost to a small business in the UK of their worst security breach of the year is £35,000 – £65,000. This is £450,000 – £850,000 for large organisations. The cost to the UK runs into billions and has 'roughly tripled over the last year'.[1] According to the 2013 Serious and Organised Crime Strategy, based on the evidence available the costs of cyber crime in the UK are likely to be a least several billions of pounds each year.[2]

4.4 A report published by RAND Europe for the Swedish National Defence College in 2013 noted that, in the last five years, for countries including Canada, Denmark, Estonia, France, The Netherlands, Russian Federation, the UK, and the US (countries for which information was available) the cyber-security threat had been prioritised in the top-tier of security issues, according to their national risk assessments.[3]

---

1 PWC 2013 Information security breaches survey, Executive Summary. http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf retrieved 01 August 2013.

2 *Serious and Organised Crime Strategy*, (CM 8715), HM Government, 2013, London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf retrieved 07 October 2013.

3 Robinson et al, Cyber-security threat characterisation – A rapid comparative analysis, RAND Europe, 2013 http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.sum.pdf retrieved 03 October 2013.

Box 4A: The threat from cyberspace

It is not just criminals who are interested in using cyberspace for financial gain. Foreign states are interested in the confidential commercial information owned and stored by British businesses. In the following extract from an interview with the BBC's Gordon Corera, an MI5 officer discussed, for the first time, the nature of these cyber attacks[1].

Gordon Corera: "The job of Britain's Security Service MI5 is not just to defend Britain against terrorist threats, but also cyber attacks. At their MI5 HQ [the] head of cyber who asked not to be named chooses his words carefully. This is the first time he has talked about it in public."

MI5 officer: "It covers all the sectors, there are now three certainties in life, there's death, there's taxes, and there's a foreign intelligence service on your system".

Gordon Corera: "Britain's under attack in that sense"

MI5 officer: "I don't think it's just the UK, this is a global widespread problem. There are hostile foreign states out there who are interested in a company's mergers and acquisitions activity, their joint venture intentions, their strategic direction over the next few years and that information would be valuable to that country's state owned enterprises."

[1] The Documentary – Under Attack: The Threat from Cyberspace, Gordon Corera, Broadcast on BBC World Service, 10:06PM Sun, 21 Jul 2013, http://www.bbc.co.uk/iplayer/episode/p01c3jxs/The_Documentary_Under_Attack_The_Threat_from_Cyberspace/ retrieved 27 July 2013.

4.5 The UK cyber strategy[4] describes in detail the nature of the threat and establishes a vision for how it will be tackled. Dealing with this threat requires a range of activities across the public as well as the private sector. All parts of the UK benefit from this strategy which is based on four objectives:

- Tackling cyber crime and making the UK one of the safest places to do business in cyberspace;
- Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace;
- Helping to shape an open, vibrant and stable cyberspace which the UK public can safely use and that supports open societies; and
- Building the UK's cross-cutting knowledge, skills and capability to underpin all of our cyberspace objectives.

4.6 As a result of the 2010 Strategic Defence and Security Review,[5] the UK Government put in place a National Cyber Security Programme (NCSP) worth £860 million over five years (2011-2016) to deliver this strategy. This is in addition to the £2 billion the security

[4] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, HM Government, November 2011 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf retrieved August 2013.

[5] *A Strong Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, HM Government, 2010, London: The Stationery Office.

and intelligence agencies receive each year.[6] In its December 2012 annual report[7] to Parliament, the Government noted that HMRC's enhanced anti-phishing capabilities were leading to the interception of 5 major threats a day, while their new cyber team had shut down almost 1,000 fraudulent websites in the previous 12 months. Over the same period, the National Fraud Authority's *Action Fraud* reporting tool had taken over 46,000 reports from the public of cyber-enabled crime. This amounted to attempted levels of fraud of £292 million. Operating on a 24/7 basis, it enables incidents of crime to be developed into intelligence packages that law enforcement agencies across the UK can use for targeted enforcement activity.

Box 4B: The UK cyber security strategy: Landscape review

According to the National Audit Office, the Serious Organised Crime Agency has repatriated more than 2.3 million items of compromised card payment details to the financial sector in the UK and internationally since 2011, preventing a potential economic loss of more than £500 million.[1]

[1] The UK cyber security strategy: Landscape review, National Audit Office, 2013 http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

4.7 Sir Iain Lobban, Director of GCHQ, stated in October 2010 that 'getting cyber right enables the UK's continuing economic prosperity'.[8] According to the International Institute for Security Studies '...addressing cyber threats in a comprehensive manner can give businesses the confidence to base in a location, knowing they can use modern IT infrastructure and reduce risk'.[9]

4.8 An independent Scottish state would no longer be covered by the UK's National Cyber Security Programme. This is because of the important role that UK Government Departments and the security and intelligence agencies play in the UK's cyber security. Given the significant risk of cyber attack recognised by the NSS, and by other countries such as those referred in the RAND Europe report described in paragraph 4.4, the Scottish Government will need to consider how to deal with this matter.

4.9 Staff retention is an issue within the UK's security and intelligence community and across all Agencies.[10] In the case of GCHQ this is because of the competition for qualified cyber specialists with the private sector.[11] Resourcing a Scotland-only capability may prove difficult given the competition for highly-skilled and scarce resources, and the loss of economies of scale mean that, within a realistic budget, an independent Scottish state may not replicate the effectiveness of current UK-wide approaches.

[6] ISC Annual Report 2012-13: http://isc.independent.gov.uk/files/2012-2013_ISC_AR.pdf retrieved 01 August 2013.

[7] UK Cyber Security Strategy: 3 December 2012 – One Year On; www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf, retrieved 03 April 2013.

[8] Sir Iain Lobban, Director GCHQ, Cyber speech to the International Institute for Security Studies, 12 October 2010. http://www.gchq.gov.uk/Press/Pages/IISS-CyberSpeech.aspx retrieved 13 Dec 2012.

[9] P.27 *Cyberspace: assessing the military dimension* in The Military Balance 2011, International Institute for Strategic Studies.

[10] Page 67, Chief of the SIS – Oral evidence before the ISC referenced in the ISC Annual Report 2011-12, July 2012.

[11] ISC Annual Report 2012-13. HC547 http://isc.independent.gov.uk/files/2012-2013_ISC_AR.pdf retrieved 01 August 2013.

Box 4C: The 2007 cyber attack on Estonia

In 2007 Estonia – one of the most digitally connected countries in the world – was the victim of a major cyber attack. Jaak Aaviksoo, the then Defence Minister, stated: "All major commercial banks, telcos, media outlets, and names servers – the phone books of the internet – felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation."[1]

[1] Joshua Davis, Hackers Take Down The Most Wired Country In Europe, Wired Magazine, Issue 15.09, 21 August 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all retrieved 01 August 2013.

Box 4D: The UK ranked No.1 in the Cyber Power Index 2012

Research by Booz Allen Hamilton and the Economist Intelligence Unit shows that the UK leads other G20 countries in its ability to withstand cyber attacks and to develop a strong digital economy.[1]

[1] Booz Allen Hamilton and the Economist Intelligence Unit, *The Cyber Power Index 2012*, January 2012, available at: www.cyberhub.com quoted in The UK cyber security strategy: Landscape review, National Audit Office, 2013 http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf retrieved 04 October 2013.

4.10 An independent Scottish state may opt to pursue the possibility of procuring cyber security services from other countries. It may also choose to look to NATO for advice. The former may help overcome the challenge of recruiting and training experts in the short term, but it would not be without risks. These include loss of control over national security systems and the protection of other assets to another country, as well as loss of control over the supply chain. An independent Scottish state would therefore still need to establish basic cyber defences to protect its own sovereignty and economy first. To do that, it would have to determine precisely what its minimum "intelligent customer"[12] capability requirement would be – its irreducible minimum.

4.11 In their report on the foreign policy implications of Scottish independence the Foreign Affairs Committee stated: "Professor Omand told us that 'the highest standards of cyber-security will be necessary for economic reasons. I cannot imagine a Government in Edinburgh would want to take a different view, [which] means you then have to have access to technical capability linked to some serious intelligence capability". Professor Omand concluded that overall, "it is not self-evident to me that that goal can be met, or that it can be met at reasonable cost".[13]

4.12 As a member of the UK however, Scotland, along with England, Wales and Northern Ireland, would continue to benefit from a range of capabilities and a comprehensive programme and investment to meet the challenges identified in the National Security Strategy. These capabilities will ensure that no part of the UK falls behind any other.

[12] Section 3.3.2 *Being an intelligent customer*, in National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security, Ministry of Defence, CM 8278, February 2012 http://www.official-documents.gov.uk/document/cm82/8278/8278.pdf retrieved 14 August 2013.

[13] House of Commons Foreign Affairs Select Committee – Sixth Report – Foreign policy considerations for the UK and Scotland in the event of Scotland becoming an independent country (1 May 2013). HC 643, London, TSO, para. 129. http://www.publications.parliament.uk/pa/cm201213/cmselect/cmfaff/643/64302.htm retrieved August 2013

Box 4E: Engagement with, and support for, the UK's security industry

A strong and competitive UK security industry is vital to our national security and in particular to the success of CONTEST in this country and overseas.

The February 2012 the UK Government Defence and Security White Paper, 'National Security through Technology', noted the contribution of the industry to developing and sustaining key security capabilities, as well as contributing to export-led growth and a balanced economy. A well-regulated trade in security products can support our strategic relationships around the world and enhance the counter-terrorism capability of our allies. The Defence and Security White Paper also recognised that exports can reduce the costs of programmes to the UK and improve the long-term viability of our own suppliers.

The global security market is increasing rapidly. It was estimated to be £410 billion in 2012 (£384 billion in 2011) and forecast to rise to £571 billion in 2016 through expected average annual growth of 9 per cent. The global export market in 2012 was estimated to be £64 billion, a rise of 3 per cent on 2011. In 2012, UK Security exports were valued at £2.7 billion, compared to defence exports which were valued at £8.8 billion.[1]

Scottish Enterprise estimates the security and resilience industry in Scotland employs 2,000 people, has sales of over £200 million, and comprises over 100 companies with products, services and applications in areas as diverse as cyber security, surveillance, business continuity and biometrics.[2]

The UK security industry has a strong reputation, not least because the UK has faced significant terrorist threats for a number of years and the industry is a key supplier to Government and the police. London 2012 further enhanced the reputation of the UK Government and industry working in partnership.

In the White Paper the Government committed to increasing support for our security industry, recognising that responsibilities in this area have historically been dispersed across Government. The Home Office has now been given the task of co-ordinating this effort in close conjunction with the Foreign and Commonwealth Office, UK Trade and Investment (UKTI) and others.

The UK Government is therefore, promoting the UK's security industry with overseas partners in an effort to increase exports. One option being explored is for the UK Government to contract directly with an overseas government through which it could prioritise UK industry as the supplier of security technologies and capabilities. One of the risks that comes with the establishment of an independent Scottish state is that Scotland would lose the benefits of the efforts the Government makes to promote the UK's security industry. Neither would its industry benefit from contracts flowing from any UK-negotiated government-to-government agreements. In a competitive international market, the benefits of scale and capability that the UK currently delivers for Scotland's security companies – as an integral part of the UK's economy – would be lost.

---

1 The figures for UK defence export orders are drawn from a survey conducted by UKTI DSO and the results published on the UKTI website. The data for UK security sector export sales is drawn from the K-Matrix report *UK Security Sector Report for 2012* on Global Security sales published in May 2013.

2 Security and resilience industry in Scotland, Scottish Enterprise, www.scottish-enterprise.com/your-sector/aerospace-defence-and-marine/adm-strategy/adm-facts/security-facts.aspx retrieved 17 May 2013.

Security of government information

4.13 The UK has in place well-established arrangements for the protection of Government assets (including information and people). The Cabinet Office is responsible for HMG's protective security policy, set out in the Security Policy Framework.[14] All departments, agencies and authorised contractors are required to put in place appropriate measures to provide the necessary level of protection against prevailing threats.

4.14 As part of this work, departments and agencies seek advice from the security authorities (the Centre for the Protection of National Infrastructure and CESG) and take part in the policy making process. Departments and agencies hold, receive, transmit and store UK protectively marked information in accordance with standards set by the Cabinet Office.

4.15 With regard to access to the most sensitive information, the UK has in place a system of security vetting. This relies, in part, on information and advice provided by the Security Service. The UK levels of security vetting clearance have equivalences within international organisations, including NATO and the EU.

4.16 Where the UK exchanges classified information with other countries, such arrangements can be formally established by a General Security Agreement (GSA): GSAs are legally binding treaties which provide the necessary assurances that information exchanged will be protected to the required standards.[15] An independent Scottish state would not be party to such GSAs negotiated and concluded by the UK. An independent Scottish state would need to consider whether it wished to pursue membership of international organisations, and meet the protective security requirements for membership.

Incident management

4.17 The likelihood of terrorists obtaining effective mass impact biological agents or a functioning radiological or nuclear device remains low, but if terrorist groups were able to use such devices successfully (as they aspire to do) their potential impact on the UK population and national infrastructure would be severe and significantly greater than a conventional terrorist attack.

4.18 After 9/11 the UK developed what it considered to be the "Model Response", i.e. the multi-agency capability to successfully respond to, and mitigate against, a Chemical, Biological, Radiological or Nuclear (CBRN) terrorist attack. The nature of this "Model Response" is classified. However, the work that resulted from the programme, applicable across the UK, has delivered the following capabilities which are available for the benefit of each and every part of the UK.

4.19 The national CBRN response centre, run by the police but available to other emergency services,[16] has delivered a range of CBRN response equipment and met its target of having over 10,000 police officers trained to respond to CBR incidents by 2010. A good level of preparedness is now provided at local and regional level through 18 'model

[14] https://www.gov.uk/government/publications/security-policy-framework retrieved 7 March 2013.

[15] GSAs are formal bilateral treaties negotiated where there is an established requirement to frequently exchange classified information between two nations. As these treaties are between the UK and other countries it follows that if Scotland left the UK the treaty would no longer apply to them.

[16] The Police National CBRN Centre is a UK-wide centre of excellence wholly owned and paid for by the Home Office. The other emergency services are represented and included in its work. It both develops doctrine and policy as well as running training courses for the emergency services.

response' teams.[17] The Police National CBRN Centre also offers a 24/7 Operations Centre to support the police with any incidents or queries where specialist advice is required, anywhere in the UK.

4.20 The National Network of Laboratories (NNL), funded by the UK Government, ensures that scientific and forensic expertise is sustained and made available to the UK emergency services for chemical and biological threats; and through other specialist MOD capabilities such as the Atomic Weapons Establishment for radiological and nuclear related threats.

4.21 The UK Government also maintains, at the MOD, a Technical Response Force (TRF) to provide specialist support to the UK police in the event of a CBRN and explosives related emergency. This enables them to both manage the incident or device, as well as to access highly specialist scientific response teams at short notice. The TRF capabilities enable a fast, consistent response across the whole of the UK.

Box 4F: What UK Government funded specialist capabilities deliver

A radiological and nuclear (RN) detection system exists at the UK border. The UK's detection capability screens traffic, people and goods to detect and deter the illicit importation of radioactive and nuclear material, reducing the risk of a terrorist RN attack in the UK. A fixed and mobile RN detection capability is operational at many major ports of entry across the UK.

Resilience and civil protection

4.22 An important part of delivering the National Security Strategy is work to mitigate the impact of serious security and civil emergency incidents in the UK. These are known as resilience capabilities, and are designed to save lives, reduce harm and aid the restoration of normality. Whilst resilience planning in the UK is structured around national legislative and doctrinal frameworks, the vast majority of resilience capabilities are locally owned and commanded, and may not be affected by the establishment of an independent Scottish state.

4.23 However, where there are national assets or capabilities owned and strategically managed by the UK Government, such as those for CBRN incidents (see above) and niche scientific capabilities such as the Government Decontamination Service,[18] access would need to be negotiated with the UK Government and new international mutual-aid agreements may be required. Access to international mutual aid for civil protection will be an important aspect of any negotiations on the terms of membership for an independent Scottish state of the EU and NATO.

4.24 Resilience preparations in the UK are founded on the principles of Integrated Emergency Management – a key component of which is risk assessment. An independent Scottish state would not have an automatic entitlement to access restricted assessments of risks and their consequences, such as the annual National Risk Assessment and other UK Government risk assessment products which are crucial to scoping and prioritising

[17] *CONTEST: The United Kingdom Strategy for Countering Terrorism*, HM Government, 2011, London, The Stationery Office, page 97.

[18] The UK Government Decontamination Service is provided by The Food and Environment Research Agency. The service helps the UK prepare for the recovery following a deliberate act involving chemical, biological, radiological and nuclear (CBRN) materials, or an accidental release of hazardous materials (HAZMAT) in excess of local capability and/or knowledge. http://www.fera.defra.gov.uk/environment/governmentDecontaminationService/index.cfm/# retrieved 15 March 2013.

resilience planning. Additionally, military assets form a small but significant part of UK resilience plans under the Military Aid to the Civil Authorities provisions. This is considered in more detail in *Scotland analysis: Defence*.

Border security

4.25 While borders will be considered elsewhere in the Scotland analysis series, border security plays an important role in safeguarding the UK's national security and in countering terrorism. There are therefore aspects of border policy that overlap with the scope of this paper. The NSS recognised the threat to the border from a significant increase in the level of terrorists, organised criminals, illegal immigrants and illicit goods trying to enter the UK. The 2010 Strategic Defence and Security Review included a commitment to make changes to pre-departure checks to better identify people who pose a terrorist threat and prevent them flying to or from the UK.[19] The Home Secretary has the power to exclude or deport individuals from the UK on grounds of national security, and the visa regime can be used as a means of preventing the travel of those who pose a security or terrorist threat. However, the visa regime is only applicable to those nationals who require a visa to travel to (or to transit) the UK.

4.26 The Pre-Departure Checks Scheme (PDCS), which has been developed by the UK Government, comprises a range of activity including; a statutory Security and Travel Bans Authority to Carry Scheme 2012 in respect of specified foreign national passengers seeking to travel to the UK; use of directions under the Aviation Security Act 1982 to prevent boarding by British nationals assessed to pose a direct threat to aircraft; and alerts to ports police to intercept individuals intending to travel in breach of terrorism-related legal restrictions outbound from the UK. The PDCS is operated by the National Border Targeting Centre (NBTC) which sends an alert to an airline or to ports police when there is a positive match to a subject of the PDCS List against advance passenger information provided by the airlines.

4.27 The Nationality, Immigration and Asylum Act 2002 (Authority to Carry) Regulations 2012 (SI 2012/1894) create a civil penalty regime applicable where an air passenger carrier either fails, without reasonable excuse, to seek authority to carry an individual specified in the Security and Travel Bans Authority to Carry Scheme 2012, or carries a person they were denied authority to carry. The provision of passenger data constitutes a request for authority to carry those passengers who are within the scope of the scheme. Where NBTC identify a positive match with a subject of the PDCS List, the carrier will be notified of a refusal of authority to carry.

4.28 As a part of the UK, Scotland – along with the rest of the UK – benefits from a robust framework for both policy development and delivery of national security at the border. A newly established independent Scottish state would need to devise its own policies and capabilities and resource their implementation, including a separate air passenger security regime for both Scottish and non-Scottish nationals. The UK would adapt to these circumstances to take account of a new international border.

[19] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, London, The Stationery Office, page 54.

Conclusion

4.29 By investing in a range of UK-wide specialist capabilities to address a range of very challenging risks related to cyber threats, the effects of a CBRN attack and border security, Scotland and every other part of the UK benefits, with no part being left behind regardless of where and when those risks may materialise.

Chapter 5: Conclusion

The current national security arrangements within the UK serve Scotland well. The analysis in this paper demonstrates that membership of the UK confers significant security benefits to the people of Scotland.

The threats that the UK faces are also faced by many other countries – large and small, far away and close to home. Countries that the current Scottish Government has cited as examples which they would want to emulate in the event of independence have unfortunately themselves experienced manifestations of the risks identified in the UK's National Security Strategy.

That is why the UK's security and intelligence agencies, and organisations responsible for undertaking intelligence analysis, work hard domestically and internationally to keep British citizens safe. They do so fully respecting the devolved nature of the police in Scotland, with whom they work closely, to pursue terrorists. They also continue to work to counter the ever present danger of espionage – human and cyber – and the threat from the spread of weapons of mass destruction and CBRN materials. These organisations would continue to operate on behalf of the continuing UK and would have no responsibility for Scotland.

The benefits of the UK do not end there. The UK has a functioning and effective system for ensuring that suspected criminals are investigated and brought to trial while respecting the history and culture of the different legal and policing traditions across the UK. This is in contrast to the bureaucratic processes in place between EU states, whether in the gathering of evidence or the arrest and detention of suspects. At the same time, current arrangements ensure that police support can be brought to bear rapidly anywhere in the UK in response to a crisis.

Efforts to counter serious and organised crime build on these institutions. The analysis in this paper demonstrates that Scotland within the UK is better placed to combat serious and organised crime because it can enjoy the best of both worlds: devolved policing in the form of Police Scotland combined with an NCA that works to the Scottish Government's organised crime strategy to ensure that serious organised criminals within Scotland, as well as those across the UK and overseas who impact on its interests, are brought to justice. An independent Scottish state would lose guaranteed access to the NCA's Intelligence Hub, its network of overseas liaison officers and specialist capabilities. These losses to Scotland would be out of proportion both to what it would have to invest to establish its own capabilities, and to what it currently contributes financially.

The loss of economies of scale would also be felt with respect to the capabilities an independent Scottish state would have to invest in regarding resilience planning. It would have to make choices about the capabilities it would seek that are currently funded by the UK. These include ensuring cyber security to safeguard its business interests and intellectual property, responding to CBRN incidents, and both initial police responses and capabilities currently funded by the UK Government and provided by the Ministry of Defence.

Introducing a new independent Scottish national security regime would both have one-off transition costs and ongoing maintenance costs. It would be very difficult to build and sustain the levels of specialist expertise and experience needed. The proposed £2.5 billion budget for both security and defence would buy only limited capabilities and Scotland would lose the benefits from the economies of scale in the existing UK-wide arrangements. Inevitably, an independent Scottish state would have less international reach and be a less attractive international partner than the current or continuing UK. Independence would put at risk access to the intelligence and other security information and networks Scotland currently enjoys as part of the UK.

Annex A:
International comparative data on the Nordic and Irish security and intelligence services

Country	Population[1]	National Security Organisations	Role
Denmark	5,556,452	PET, Danish Police Security and Intelligence Service	Responsible for dealing with internal security issues and those that threaten Danish interests/citizens overseas.[2]
		DDIS, Danish Defence and Intelligence Service	Denmark's foreign intelligence and military intelligence service.[3]
Finland	5,266,114	Finland Security Intelligence Service (Police)	Responsible for counter terrorism and counter espionage.[4]
Ireland	4,775,982	An Garda Siochána	Responsible for ensuring national security including against terrorism and organised crime.
		Irish Defence Forces	Responsible for military intelligence.
Norway	4,722,701	Police Security Service (PST)	Responsible for dealing with domestic security threats.
		External Service (NIS)	Responsible for dealing with overseas threats to national security.
		National Security Authority	Responsible for dealing with cyber threats.[5]
Sweden	9,119,423	SÄPO, Swedish Security Police	Responsible for dealing with domestic security threats – counter espionage, counter terrorism, counter subversion, protective security and dignitary protection.[6]
		MUST, Swedish Military Intelligence	Responsible for overseas threats to national security.
		FRA, Sweden's Signals Intelligence Agency	Responsible for signals intelligence and Information Assurance.[7]
United Kingdom	63,700,000	The Security Service (MI5)	Responsible for protecting the UK against threats to national security from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
		Secret Intelligence Service (SIS)	Collects secret intelligence and mounts covert operations overseas in support of British Government objectives.
		Government Communications Headquarters (GCHQ)	Responsible for gathering intelligence through the monitoring of communications, and providing services and advice as the UK's authority for Information Assurance.
		Defence Intelligence	Responsible for support to operations, support to contingency planning, provision of early warning of impending crises around the world and analysis of emerging threats.

1 All population figures (except UK) taken from CIA World Factbook, http://cia.gov/library/publications/the-world-factbook/index.html retrieved 23 Oct 2013. UK figures taken from Office for National Statistics *Population Estimates for UK, England and Wales, Scotland and Northern Ireland, Mid-2011 and Mid-2012*, http://www.ons.gov.uk/ons/rel/pop-estimate/population-estimates-for-uk--england-and-wales--scotland-and-northern-ireland/mid-2011-and-mid-2012/index.html retrived 10 Oct 2013.

2 PET, 'About PET', https://www.pet.dk/English/About%20PET.aspx?p=1 retrieved 30 August 2013.

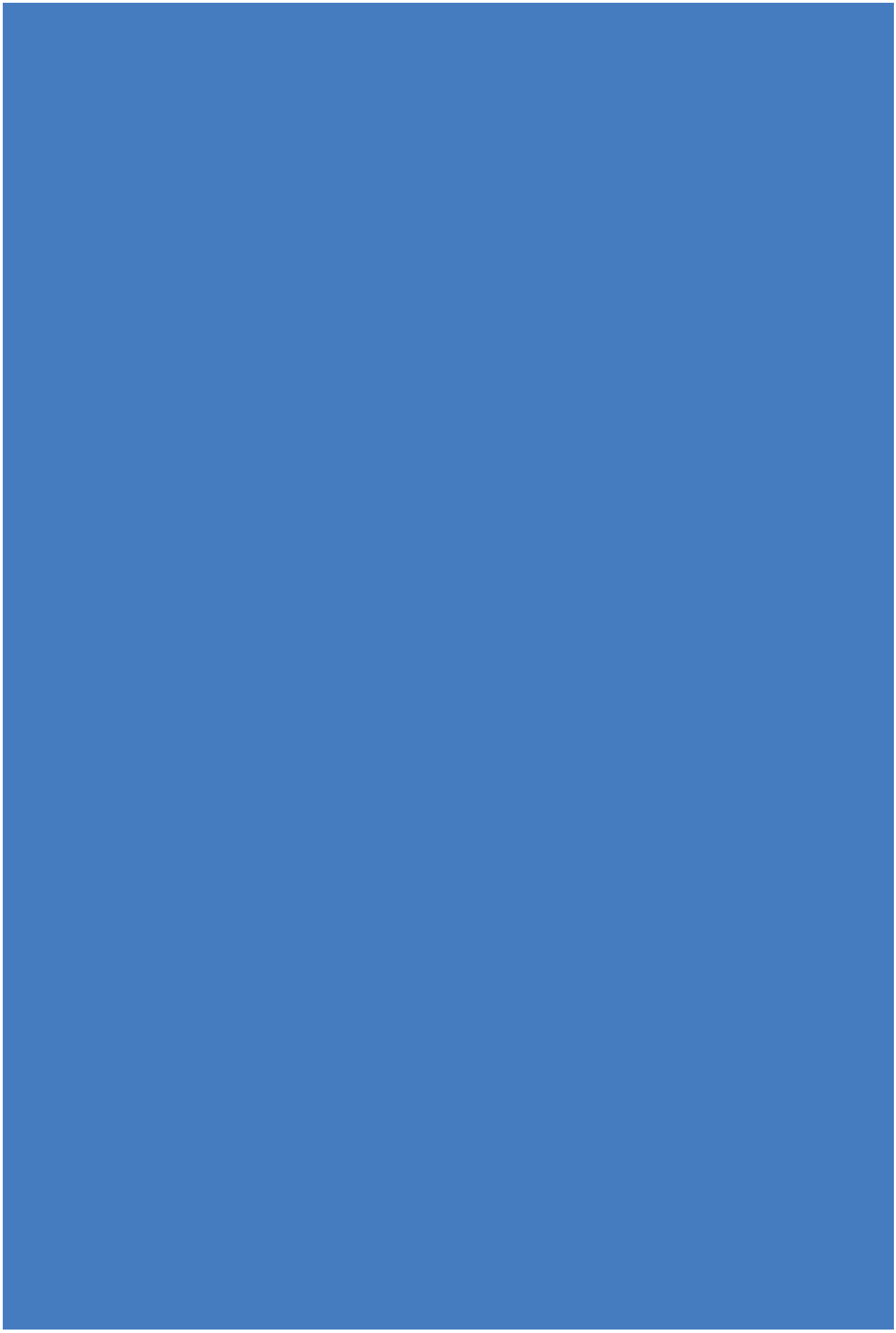
3 DDIS, 'About DDIS', http://fe-ddis.dk/eng/About-DDIS/Pages/About-DDIS.aspx retrieved 30 August 2013.

4 Finnish Security Intelligence Service – www.poliisi.fi/poliisi/supo60/home.nsf/pages/indexeng retrieved 30 August 2013.

5 National Security Authority, https://www.nsm.stat.no/Engelsk-start-side/About-NSM/ retrieved 30 August 2013.

6 Swedish Security Service (Säkerhetspolisen), http://www.securityservice.se/english/english.4.3b063add1101207dd46800058538.html retrieved 30 August 2013.

7 FRA, http://fra.se/snabblankar/english.10.html retrieved 30 August 2013.



Annex B: National Crime Agency Specialist Capabilities

Examples of National Crime Agency national capabilities which an independent Scottish state would have to consider whether to invest to retain or replicate include:

- **The Child Exploitation and Online Protection Command (CEOP)**

  Scotland benefits from a UK perspective in terms of intelligence received, knowledge shared and best practice pursued. For example, a total of 157 intelligence records were disseminated by CEOP to Scottish policing partners during the calendar year of 2012. CEOP has also instituted a regional point of contact with Scotland in order to provide assistance, advice and co-operation.

- **UK Human Trafficking Centre (UKHTC)**, including running the National Referral Mechanism.[8] The UKHTC, within the Organised Crime Command, provides a central point for the development of expertise and co-operation in relation to the trafficking of human beings. It provides tactical advice and specialist support to UK police forces and other stakeholders from the governmental, non-governmental and inter-governmental sectors.

- **UK Financial Intelligence Unit (UKFIU)**

  The UKFIU administers the suspicious activity reports (SARs) regime, the end-to-end system by which industry identifies suspicious activity related to money laundering and terrorist financing and reports it to the NCA. These reports are available to law enforcement agencies to use to tackle crime and terrorism. UKFIU activity includes engaging with industry reporters. A national FIU is a requirement of EU Regulation and international standards.[9]

- **UK National Central Office for Counterfeit Currency**
  The NCA contains the designated national central office for the suppression of counterfeit currency. The Operational Support Team provides leadership, coordination and expertise to UK Law Enforcement investigating counterfeit currency offences, and collates, develops and acts upon intelligence from UK and international agencies regarding significant OCGs involved in counterfeit currency impacting on the UK. The Analysis Team processes and classifies currency believed to be counterfeit from all UK police forces, the Scottish, Northern Irish cash centres and bureaux de change.

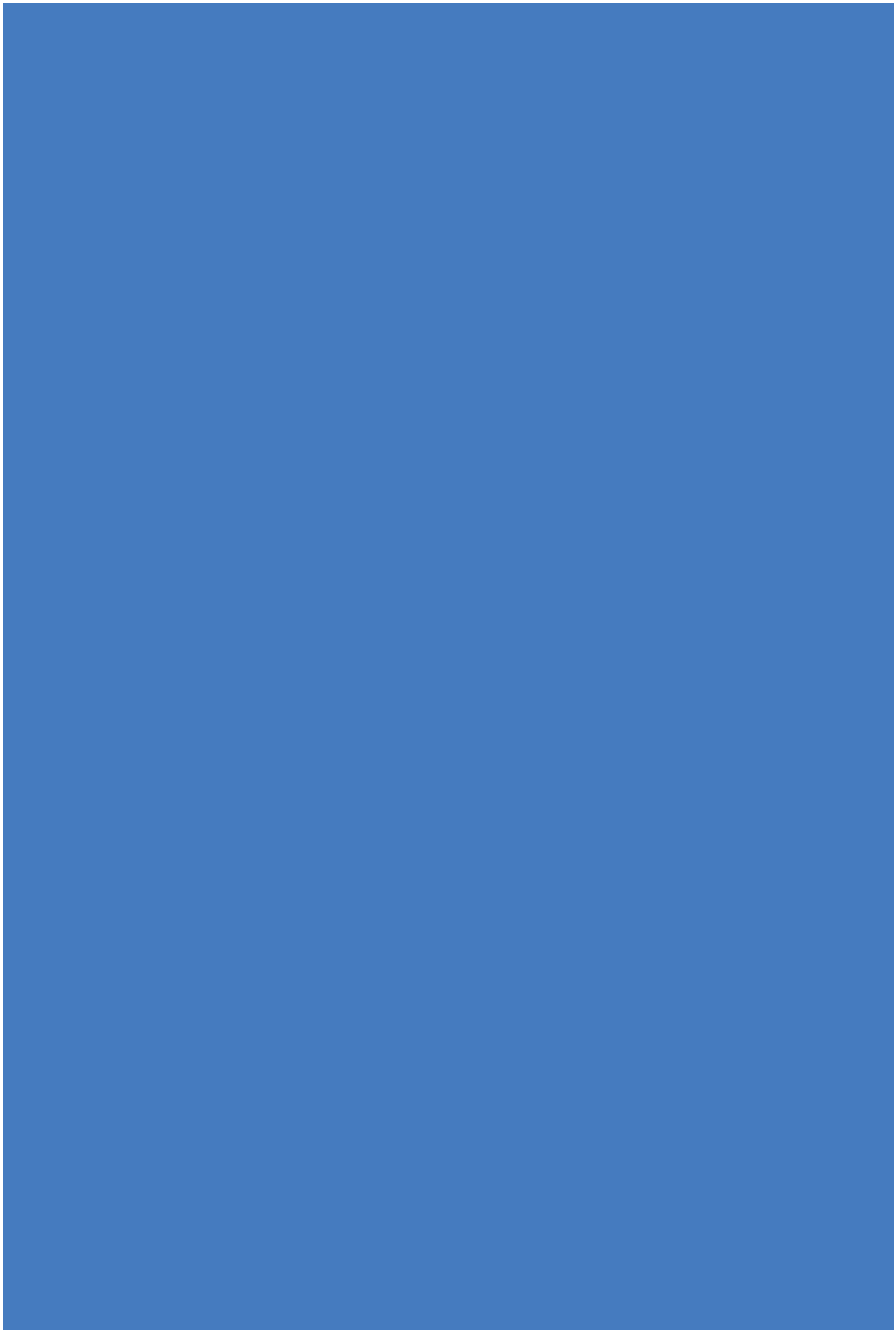
---

[8] The National Referral Mechanism (NRM) was introduced in 2009 to meet the UK's obligations under the Council of European Convention on Action against Trafficking in Human Beings.

[9] Article 21, Third EU Money Laundering Directive

- **Missing persons bureau**
  The MPB is the UK national and international point of contact for all missing persons and unidentified body cases. It works alongside police forces and other related organisations, seeking to improve both the efficiency and effectiveness of missing person investigations.
- **Anti-Kidnap and Extortion Unit**
  The Anti-Kidnap and Extortion Unit provides operational support and strategic and tactical advice to police forces and other agencies, both in the UK and overseas. It also provides kidnap training and exercises to UK partner agencies, including those in Scotland.
- **Serious Crime Analysis Section (SCAS)**
  The SCAS team of crime analysts and specialist officers analyses rape and serious sexual assaults, and motiveless or sexually motivated murder cases. SCAS receives case files from a network of contact officers employed in intelligence departments in every police force in the UK.
- **Specialist Operations Centre (SOC)**
  The SOC provides UK policing with information, advice and support in relation to surveillance law, major crime and vulnerable and intimidated witnesses in four key areas: specialist research, covert advice, witness intermediary and crime.
- **Crime Operational Support**
  Crime Operational Support provides expert assistance to police forces dealing with serious crime investigations (including murder, rape, series and serious sexual offences, abduction, suspicious missing persons and no body murder investigations).
- **Illicit Laboratory Team**
  The team provides forensic services throughout the UK in relation to the investigation of synthetic drugs production and operations which may include hazardous environments.
- **Interpol / Europol liaison**
  While Police Scotland has the ability to undertake Interpol/Europol checks they call upon the NCA's bureau services in a surge capacity.
- **Specialist cyber support**
  Police Scotland has cyber capabilities but can draw upon the specialist cyber capabilities of the National Cyber Crime Unit as needed.
- **Technical collection**
  The Scottish Recording Centre provides intercept services to Scottish partners. The NCA also provides Scottish forces with access to intercept material it has collected relating to criminal activity impacting on Scotland – although the activity may have occurred or the material been collected outside Scotland. The NCA technical collection team can also provide additional assistance to supplement Police Scotland's capabilities when needed.
- **Technical Operations Support**
  Although Police Scotland has its own capability, NCA Technical Operation Support are utilised for sensitive operations.

- **Specialist surveillance**
  Police Scotland has its own specialist surveillance capabilities, but can draw upon those capabilities within the NCA on a surge basis or as additional capabilities are required.



Bibliography

Allardyce J, Support for solo Scotland waning, The Sunday Times, 27 January 2013 (behind pay wall). http://www.thesundaytimes.co.uk/sto/news/uk_news/scotland/article1202537.ece retrieved August 2013.

Bradley J, 'Cyber crime costs Scots businesses £160 a second', The Scotsman 25 June 2013 http://www.scotsman.com/the-scotsman-2-7475/scotland/cyber-crime-costs-scots-businesses-160-a-second-1-2974653 retrieved August 2013.

Cabinet Office (Nov. 2012) *Annual Report on the National Security Strategy and Strategic Defence and Security Review* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83775/121128-Annual-Report-to-Parliament-on-NSS-and-SDSR.pdf, retrieved August 2013.

Cabinet Office, National Intelligence Machinery Booklet (Nov 2010), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf retrieved August 2013.

Cabinet Office, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, November 2011 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf retrieved August 2013.

Cabinet Office, UK Cyber Security Strategy: 3 December 2012 – One Year On www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf, retrieved 03 April 2013.

Chalmers M, The End of an 'Auld Sang' Defence in an Independent Scotland, RUSI briefing paper, April 2013 http://www.rusi.org/downloads/assets/End_of_an_Auld_Sang.pdf retrieved August 2013.

CIA World Data Factbook, http://cia.gov/library/publications/the-world-factbook/index.html retrieved January 2013.

Corera G, The Documentary – Under Attack: The Threat from Cyberspace, Broadcast on BBC World Service, 10:06PM Sun, 21 Jul 2013. http://www.bbc.co.uk/iplayer/episode/p01c3jxs/The_Documentary_Under_Attack_The_Threat_from_Cyberspace/ retrieved July 2013.

Council of the European Union, Replies to questionnaire on quantitative information on the practical operation of the European arrest warrant – Year 2010, document 9120/2/11 REV 2, 9 September 2011. http://register.consilium.europa.eu/pdf/en/11/st09/st09120-re02.en11.pdf retrieved August 2013.

Crime (International Co-operation) Act 2003 http://www.legislation.gov.uk/ukpga/2003/32/contents retrieved August 2013.

Cross-border enforcement, CPS website http://www.cps.gov.uk/legal/v_to_z/withdrawal_of_bench_warrants/ retrieved August 2013.

Cyberspace: assessing the military dimension in The Military Balance 2011, International Institute for Security Studies.

Davis J, Hackers Take Down The Most Wired Country In Europe, Wired Magazine, Issue 15.09, 21 August 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all retrieved August 2013.

Evans J, Director General – Security Service, Address to the Worshipful Company of Security Professionals, 16 September 2010. https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-threat-to-national-security.html retrieved August 2013.

Foreign Affairs Committee - Sixth Report – Foreign policy considerations for the UK and Scotland in the event of Scotland becoming an independent country (1 May 2013). HC 643, London, The Stationery Office. http://www.publications.parliament.uk/pa/cm201213/cmselect/cmfaff/643/64302.htm retrieved August 2013.

Grant G, *In Scotland's Defence? An Assessment of SNP Defence Strategy*, Henry Jackson Society. July 2013.

HM Government (2010), *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* London: The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf retrieved August 2013.

HM Government (2010), *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* London: The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf retrieved August 2013.

HM Government (July 2011) *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf retrieved August 2013.

HM Government (March 2013), *The United Kingdom's Strategy for Countering Terrorism Annual Report*, London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_Cm_8583_v0_20.pdf retrieved August 2013

HM Government (2013), *Serious and Organised Crime Strategy*, (CM 8715) London, The Stationery Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf retrieved October 2013.

Home Office Research Report 73 (2013) *Understanding Organised Crime: Estimating the scale and the social and economic costs,* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr73.pdf retrieved October 2013

House of Lords European Union Committee, Justice, Institutions and Consumer Protection Sub-Committee, Home Affairs, Health And Education Sub-Committee, regarding the UK's 2014 Opt-Out Decision ('Protocol 36') , Oral and Written Evidence, http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/Protocol36OptOut/VolofevidenceP36asat250313.pdf retrieved September 2013.

House of Lords, *Regina* v. Manchester Stipendiary Magistrate and the Lord Advocate (Appellants) Ex Parte Granada Television Ltd. (Respondent), 14 December 1999. http://www.publications.parliament.uk/pa/ld199900/ldjudgmt/jd991214/granad-1.htm retrieved August 2013.

Intelligence Services Act 1994, http://www.legislation.gov.uk/ukpga/1994/13/contents, retrieved August 2013.

Irish Information Security and Cybercrime Survey 2013, Deloitte / EMC http://www.deloitte.com/assets/Dcom-Ireland/Local%20Assets/Documents/ERS/2013/IE_A_ERS_Cyber%20Crime%20Survey_digi_0713.pdf retrieved August 2013.

Intelligence and Security Committee Annual Report 2012-13: http://isc.independent.gov.uk/files/2012-2013_ISC_AR.pdf retrieved August 2013.

Intelligence and Security Committee Annual Report 2011-12: http://isc.independent.gov.uk/files/2011-2012_ISC_AR.pdf retrieved August 2013.

Ministry of Defence, Operations in the UK: The Defence Contribution to Resilience, Joint Doctrine Publication 02 (JDP), 2nd Edition. September 2007 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43328/jdp02ed2.pdf retrieved August 2013.

Levitz D, EU pressures skittish member nations to store telecommunications data, 19 April 2011. http://www.dw.de/eu-pressures-skittish-member-nations-to-store-telecommunications-data/a-14998212 retrieved August 2013.

Lobban I, Director GCHQ, Cyber speech to the International Institute for Security Studies, 12 October 2010 http://www.gchq.gov.uk/Press/Pages/IISS-CyberSpeech.aspx retrieved Dec 2012.

Menn J, Cyber attacks against banks more severe than most realize, 18 May 2013, Reuters. http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518 retrieved August 2013.

Ministry of Defence, Being an intelligent customer, in *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, Ministry of Defence, CM 8278, February 2012. http://www.official-documents.gov.uk/document/cm82/8278/8278.pdf retrieved August 2013.

Mutual Aid Resources for London 2012 Olympic and Paralympic Games, Metropolitan Police Media Library. http://media.met.police.uk/documents/MutualAid.pdf retrieved August 2013.

PwC 2013 Information security breaches survey, Executive Summary http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf retrieved August 2013.

Ramsay M, Security service can take nothing for granted, Scotland on Sunday, 17 February 2013, http://www.scotsman.com/scotland-on-sunday-2-7506/opinion/comment/meta-ramsay-security-service-can-take-nothing-for-granted-1-2795918 retrieved August 2013.

Robertson A, The Case for Staying in NATO, Sunday Herald, 26 October 2012. http://www.heraldscotland.com/politics/opinion/the-case-for-staying-in-nato-by-angus-robertson.18682698 retrieved August 2013.

Sawers J, Chief of SIS, 'Britain's Secret Frontline', speech to the Society of Editors, 29 October 2010. https://www.gov.uk/government/news/britains-secret-frontline-mi6-chief-speaks-in-public-for-the-first-time retrieved August 2013.

The Scotland Institute, Defence and Security in an Independent Scotland, June 2013, http://www.scotlandinstitute.com/wp-content/uploads/2013/06/Defence_Report_-_Scot_Inst.pdf retrieved August 2013.

Security and resilience industry in Scotland, Scottish Enterprise website, www.scottish-enterprise.com/your-sector/aerospace-defence-and-marine/adm-strategy/adm-facts/security-facts.aspx retrieved 17 May 2013.

Security Service Act 1989, http://www.legislation.gov.uk/ukpga/1989/5/contents retrieved August 2013.

Summary Jurisdiction (Process) Act 1881 http://www.legislation.gov.uk/ukpga/Vict/44-45/24/contents retrieved August 2013.

Summer newsletter, Scottish Business Resilience Centre, June 2013, http://www.sbcc.org.uk/media/92421/sbrc_summer_newsletter.pdf retrieved 02 August 2013, retrieved August 2013.

The Regulation of Investigatory Powers Act 2000, http://www.legislation.gov.uk/ukpga/2000/23/contents retrieved August 2013.

The Regulation of Investigatory Powers (Scotland) Act 2000 http://www.legislation.gov.uk/asp/2000/11/contents retrieved August 2013.

Scottish National Party resolution on NATO, published in full in The Scotsman on 16 July 2012 http://www.scotsman.com/news/politics/top-stories/in-full-snp-resolution-on-nato-1-2414919 retrieved August 2013.

The Scottish Government (2009) Letting Our Communities Flourish: A Strategy for Tackling Serious Organised Crime in Scotland, Edinburgh, http://www.scotland.gov.uk/Resource/Doc/274127/0081989.pdf retrieved August 2013.

The Scottish Government (2010), Preliminary findings on the scale and extent of serious organised crime in Scotland: Scottish serious organised crime group mapping project, http://scotland.gov.uk/Resource/Doc/254429/0098144.pdf retrieved 02 September 2013.

Tayside Police, Cross Border Powers (20 September 2010), http://www.tayside.police.uk/Downloads/foi%20files/policies/Cross%20Border%20Powers.pdf retrieved December 2012.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call: 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Houses of Parliament Shop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents