TERRORISM AND EUROPEAN SECURITY GOVERNANCE
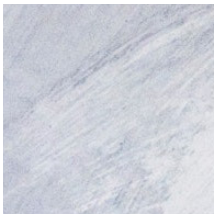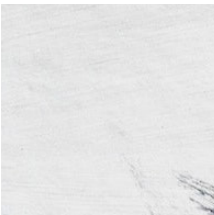
Edited by Andreas Gofas

Robert Schuman Centre for Advanced Studies

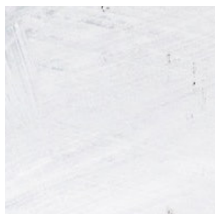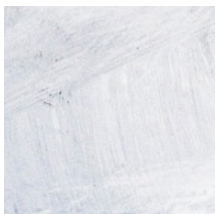The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The Global Governance Programme

The Global Governance Programme is one of the flagship programmes of the Robert Schuman Centre. It is made of a community of outstanding professors and scholars, produce high quality research and engage with the world of practice through policy dialogue. Established and early career scholars research write on and discuss issues of global governance within and beyond academia, focusing on four broad and interdisciplinary areas: Global Economics, Europe in the World, Cultural Pluralism and Global Citizenship.

The Programme also aims to contribute to the fostering of present and future generations of policy and decision makers through its executive training programme: the Academy of Global Governance, where theory and 'real world' experience meet and where leading academics, top-level officials, heads of international organisations and senior executives discuss on topical issues relating to global governance.
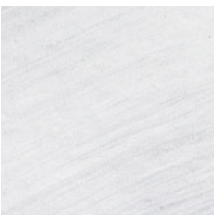
For more information: http://globalgovernanceprogramme.eui.eu

TERRORISM AND EUROPEAN SECURITY GOVERNANCE

Edited by
Andreas Gofas

TABLE OF CONTENTS

INTRODUCTION

Andreas Gofas

Associate Professor of International Relations, Panteion University of Athens; director of the Center for the Analysis of Terrorism and European Security (CATES) at the European Law and Governance School; and co-director, Olympia Summer Academy.

Terrorism, and our response to it, is among the most compelling European security issues. To expand on a point made by Richard English, we face four kinds of terrorist problem. The first is practical and the second analytical, and our difficulties in responding to the practical problem have been significantly exacerbated by our failings with regard to the analytical.[1] The third kind of terrorist problem is informational and the fourth perceptual. For many years, data-driven analysis and information regarding the terrorist risk Europe is facing have failed to reach opinion-makers and mainstream audiences. At the same time, the considerable counter-terrorism efforts made by both the EU and NATO have gone somewhat unnoticed by the European public. Indeed, according to a 2016 Special Eurobarometer survey, 69% of European citizens consider EU action in the fight against terrorism to be "insufficient."[2] In effect, the threat of terrorism remains a source of much public anxiety, with 40% of European citizens perceiving the risk of a terrorist attack to be high.[3]

In order to discuss these hugely important problems and all too pressing security governance challenges, in June 2017 the Robert Schuman Centre for Advanced Studies organised a workshop on 'Terrorism and European Security Governance.' In line with the Centre's mission to promote dialogue with the world of practice, the workshop brought together well-known academics in the field and officials from NATO, Europol and the European Commission. This edited volume groups together some of the presentations delivered at the workshop to make a minor, yet hopefully timely, contribution to the analytical and governance challenges that we face and also to the framing of the wider debate on the security situation in Europe.

I am particularly thankful to the volume's authors for their insightful contributions, to NATO's Public Diplomacy Division for co-sponsoring the event that led to this work, to the Director of the Robert Schuman Centre, Professor Brigid Laffan, for fully supporting the project from its inception, and to Professor Diego Gambetta and Professor Olivier Roy for acting as workshop panel chairs and enriching the debate.

---

1   Richard English, *Terrorism: How to Respond*. Oxford: Oxford University Press, 2009, p. ix.

2   Public Opinion Monitoring Unit, *Europeans in 2016: Perceptions and expectations, fight against terrorism and radicalization*, *Special Eurobarometer of the European Parliament*, European Parliamentary Research Service, European Commission, 2016, p. 8 (available at: http://www.europarl.europa.eu/pdf/eurobarometre/2016/attentes/eb85_1_synthesis_perceptions_wishes_terrorism_en.pdf) .

3   Ibid, p. 10.

UNDERSTANDING THE ENEMY: ANALYTICAL CHALLENGES

UNDERSTANDING TERRORISM IN THE TWENTY-FIRST CENTURY

Richard English

Professor of Politics at Queen's University Belfast, where he is also Distinguished Professorial Fellow in the Senator George J. Mitchell Institute for Global Peace, Security and Justice.

Four main points are vital when we attempt to understand twenty-first-century terrorism.

First, let us not forget what we already know that we know about terrorism; let us not overlook the knowledge that has been derived from close scrutiny of its long past. The most important areas of analysis regarding terrorism (definition, causation, consequences, best response) are all ones on which there exists a vast amount of hard-learned understanding. This does not always seem to be the case when one listens to some politicians, as they (for example) promise to eradicate from the face of the earth a form of terrorism that is almost certain to outlive their own political careers. In reality, we know that terrorism will be something with which we have to learn to live rather than something which can be extirpated; and we know that the forms of terrorism about which we are most concerned (those practised by the major enduring terrorist organizations) are themselves likely to persist for a lengthy period before disappearing. A vast literature attests to these findings.[1]

We also know that we know that intelligence-led policing in most cases offers a more powerful resource for countering terrorism than does a more militarily-focused response (although the two need not be mutually exclusive); that mistreating suspects will probably do the state's adversaries more good than it will benefit the state itself; and that credibility in counter-terrorist public argument is vital.[2]

So we need to agree on what we have cumulatively learned. This is as true of the scholarly community as it is of politicians. And it means that we have to recognize how new (or not new) some recently published arguments actually are. Marc Sageman has done much valuable work analysing terrorism,[3] but his 2017 book, *Misunderstanding Terrorism*, presents a supposedly new 'Model of the Turn to Political Violence' which is in fact already very deeply familiar from the existing literature on past terrorist campaigns. Scholars who know the histories of even older terrorist groups such as ETA, Hamas, the Provisional IRA or the Baader-Meinhof group are fully aware of the supposedly new model that Sagemen sets out of actors turning to terrorism: "escalation of hostility between the state and their community, which includes a cumulative radicalization of discourse; their disillusionment with non-violent legal tactics; and moral outrage at new state aggression against their community."[4]

1   See, for example, R. Singh, Hamas and Suicide Terrorism: Multi-Causal and Multi-Level Approaches (London: Routledge, 2011); R. English, Armed Struggle: The History of the IRA (London: Pan Macmillan, 2012 edn.); R. English, Terrorism: How to Respond (Oxford: Oxford University Press, 2009); M. Crenshaw and G. LaFree, Countering Terrorism (Washington, D.C.: Brookings Institution, 2017); A. K. Cronin, How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns (Princeton: Princeton University Press, 2009); L. Richardson, What Terrorists Want: Understanding the Terrorist Threat (London: John Murray, 2006).

2   For expansion on these points, see R. English, *Terrorism: How to Respond*. See also S. O'Mara, *Why Torture Doesn't Work: The Neuroscience of Interrogation* (Cambridge: Harvard University Press, 2015).

3   M. Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004); M. Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008).

4   M. Sageman, *Misunderstanding Terrorism* (Philadelphia: University of Pennsylvania Press, 2017), pp. 111, 130; cf. R. English, *Does Terrorism Work? A History* (Oxford: Oxford University

To forget or to ignore what we know that we know will hamper our forward movement as a scholarly community of understanding. A similar amnesia in policy circles is potentially as damaging, and has been evident in the practice of some major counter-terrorist organizations.[5]

The second point to stress is this: we need to resolve as far as we can the problem of the geography of understanding terrorism. It is a common reality that the geographical settings within which scholarly research is conducted can generate contextual biases, preferences and cultures of interpretation.[6] Such a pattern is also evident in the academic study of terrorism, in the sense that most terrorism research is carried out in settings in which there is very little terrorism, while those settings generating most terrorism produce comparatively little influential research on the subject. So, for example, a third of all terrorist attacks recorded in the Global Terrorism Database (GTD) occurred in just five countries: Colombia, India, Iraq, Pakistan and Peru; in 2012, over half of all worldwide terrorist attacks occurred in just three countries: Iraq, Pakistan and Afghanistan.[7] But if we consider the locations of the contributors to a leading journal in the field, *Terrorism and Political Violence*, we find that for the period 2000-14, 46% of the articles originated from US-based scholars, 71.5% originated from the USA, the UK and Israel, and a mere 1% involved people based in any of the five countries which account for a third of all GTD terrorist attacks (Colombia, India, Iraq, Pakistan and Peru).[8]

Now there are clear reasons for this, including the

geographically-weighted infrastructure of major universities, the dominance of English-language research, and the cultural and political barriers to the generation of academic work in some settings. I am not in any way seeking to criticize journal editors, and I do not underestimate the obstacles to remedying this problem. Nor am I suggesting that only those scholars with long-term proximity to terrorism will produce the best research. However, it does seem to me that there are some potential and distinctive insights to be gleaned from such long-term context-based immersion, and that the existing imbalance between long-distance work and field-based work perhaps occludes our vision of this phenomenon (especially since most terrorism remains local).[9] Long-term field-based expertise is also vital in terms of policy-based understanding of terrorism and counter-terrorism; and again there are occasions when such expertise seems not to be as fully appreciated as might be ideal.[10]

Third, understanding terrorism in the twenty-first century means looking simultaneously at terrorism, counter-terrorism and the mutually shaping relationship between them. There exists a paradoxically intimate relationship between state actors and their non-state terrorist adversaries, and the actions of each side help to determine the behaviour of their opponent. This has long been the case, whether in Israel/Palestine, Spain, Ireland, Colombia, Sri Lanka, Chechnya, western Europe during the late-twentieth-century era of left-wing violence, or more recently in the post-9/11 era. So the journey from al-Qaida to ISIS, for example, is one which can only be understood if we identify the effects of post-11 September counter-terrorism policy on the regional politics which helped to generate Islamic State.[11]

On both sides of this antiphonal asymmetrical

Press, 2016); S. Aust, *Baader-Meinhof: The Inside Story of the RAF* (Oxford: Oxford University Press, 2009 edn.).

5   C. Andrew, *The Defence of the Realm: The Authorized History of MI5* (London: Penguin, 2009).

6   D. N. Livingstone, *Putting Science in its Place: Geographies of Scientific Knowledge* (Chicago: University of Chicago Press, 2003).

7   G. LaFree, L. Dugan, and E. Miller, *Putting Terrorism in Context: Lessons from the Global Terrorism Database* (London: Routledge, 2015), p. 53.

8   R. English, 'The Future Study of Terrorism,' *European Journal of International Security* (1, 2, July 2016).

9   A. B. Krueger, *What Makes a Terrorist: Economics and the Roots of Terrorism* (Princeton: Princeton University Press, 2007).

10   J. Nixon, *Debriefing the President: The Interrogation of Saddam Hussein* (London: Bantam Press, 2016).

11   F. A. Gerges, *ISIS: A History* (Princeton: Princeton University Press, 2016).

relationship between terrorists and counter-terrorists there tends to be an exaggeration of what violence can achieve; and also on both sides there tends to be a comforting sense that prior violence by the other side legitimates brutality by one's own. How far this seems true will vary from case to case and from observer to observer. But the central reality remains: whether as an academic or as a policy actor, one cannot properly understand and respond to non-state terrorism without synoptically examining terrorism, counter-terrorism, and their complex protean relationship with one another.[12]

Fourth, a fuller understanding of terrorism in the twenty-first century will emerge, I believe, if historians and an appreciation of history play an increasingly major part in our thinking. The blinding power of terrorist atrocity often involves an impulse towards the solipsism of the present. So post-9/11 considerations probably over-focused on al-Qaida, just as (at time of writing) an obsession with ISIS perhaps hinders longer-term understanding and reflection.

I am not suggesting that only historians can understand and explain terrorism. Every academic discipline has the potential to offer profound and unique insights, and what we require is multi-disciplinary analysis. But it is true that historians as a tribe have been less keen to colonize the territory of terrorism than have, say, political scientists, international relations scholars or economists. It is also true that there are distinctive aspects of historians' methodology which might yield particular benefit as we reflect on this long-rooted phenomenon.

A number of elements in the historian's typical approach might be judged especially valuable. Historians assess change and continuity over lengthy pasts, and this might serve as a corrective to easy over-presentist assessments of terrorist

threats, dangers and possibilities. Historians also tend to focus on the complex particularity, and even the uniqueness, of each setting; this can help to avoid over-simplistic generalizations, an ever-present difficulty when facing terrorism. The historian's commitment to engagement with large numbers of mutually interrogating sources, including first-hand sources, helps to ensure a clear-eyed view of what terrorists actually intend and accomplish. The historians' instinctive scepticism about over-Procrustean abstract theory counters some tendencies in a theoretically model-dominated field. And the majority preference among historians for the contingent rather than the inevitable during processes of human change again counsels us against crudely determined analyses.[13]

As noted, none of this undermines the enormous and equal value of other disciplinary approaches. But there are intellectual as well as practical policy-relevant dimensions to a historically attuned approach to twenty-first-century terrorism. Not least among these will be a humility about what can actually be achieved. When one considers the historical complexity and the very long roots of terrorism-generating conflicts (from Israel/Palestine to Syria, to Iraq, to Afghanistan, to Ireland, to Colombia and beyond), one is struck by how Sisyphean a task counter-terrorism can seem. If such an attitude seems depressing, then the dangers of ignoring such a scale of challenge are probably more appalling.

<hr>

12   For wider discussion of these points, see R. English (ed.), *Illusions of Terrorism and Counter-Terrorism* (Oxford: Oxford University Press, 2015).

13   For an expansion on the ways in which historical method can aid the study of terrorism, see R. English, *Does Terrorism Work?*

THE INTERACTION BETWEEN COUNTERTERRORISM AND TERRORIST GROUPS

Isabelle Duyvesteyn

Professor of International Studies and Global History, Leiden University

What is the link between the Peruvian Shining Path, Hezbollah and Al Qaeda? The answer is that despite the very different locations, backgrounds and approaches of these groups, all feature on international lists of designated terrorist organisations.[1] This contribution will argue that grouping these divergent violent actors together under the rubric of terrorism is a problem. It is problematic not only because it muddles the definition and conceptualisation of terrorism unnecessarily through the inclusion of a panoply of different organisations with different strategic approaches but, importantly, the practice is also problematic because the diverging strategies the groups employ have important consequences and constraints on the counter-measures that states can enact. A conceptual distinction between terrorist and insurgent strategies is crucial. Political, organisational and relational distinctions separate these two distinct approaches. Making the distinction is important, first, in order to understand the widespread charge that there is too much of a Western focus in the terrorism debate to the detriment of non-Western experiences (see also the contribution by Richard

English in this volume). Second, the distinction has significant consequences when it comes to designing appropriate answers to counter these activities. This contribution will proceed by first outlining the differences between the two strategic approaches and subsequently thinking through the consequences for counterterrorism (CT).

Terrorism versus Insurgency[2]

In contemporary discourse, it appears that any non-state armed group using violence is terrorist. This simplification of reality obfuscates the fact that many of these non-state groups have a choice between several different approaches to challenge their opponents, which are usually states. Terrorism is but one of these methods. It can be distinguished from insurgency and conventional war, its two main alternatives, by its distinctive political, organisational and relational features. Politically, terrorism is an indirect approach; organisationally, it thrives on secrecy but possesses limited material and human capacity; and relationally, it is often distant from the population rather than operating in its midst. Insurgents are not simply terrorists with territory but have a distinct dynamic of their own. Their political strategy is geared towards putting direct pressure on the government or governments; this is combined with an active organisation of the population in an alternative governance relationship or a shadow state; and relationally, insurgents operate among the population on whose behalf they (claim to) fight. Conventional war is relatively rare among non-state groups since it requires large-scale material and fighting capacities that are usually the prerogative of states. The Tamil Tigers are one of the few groups that have managed to fight conventionally but this was part of a final phase of insurgency warfare. Politically,

---

1   For the US list, see https://www.state.gov/j/ct/rls/other/des/123085.htm. For the EU list, see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009E0468&qid=141259635797&from=EN.

2   For a previous version of some of these arguments, see Isabelle Duyvesteyn and Mario Fumerton 2009. 'Insurgency and Terrorism: Is there a difference?' in: Caroline Holmqvist-Jonsater and Christopher Coker (eds.), *The Character of War in the 21st Century* London: Routledge, pp. 27-41.

conventional war entails a direct translation of military goals into political ends; organisationally, it requires direct large-scale consistent engagement with the population, possibly in the shape of a social contract; relationally, there are very close ties between the group and the population. Since conventional war is rare, the elaboration of these arguments below will focus on the distinction between terrorism and insurgency.

Terrorism and insurgency both embrace a political goal. The road to achieve it, however, diverges. Contrary to some recent scholarship, this contribution will argue that terrorism is a strategic enterprise and not simply a tactic or a method. The reason is that there is a means-ends relationship, which features prominently in almost all attempts to understand this social phenomenon. If we deny the political dimension and focus solely on terrorism as a tactic, part of the picture becomes unbalanced. To be fair, within the strategic approach of insurgency, terrorism does occur as a tactic. In that case it remains linked to the means-ends relationship that is central to insurgency as well.

The essence of the strategic approach of terrorism is to provoke responses from the opponent that will bring the stated goals closer. A terrorist strategy in and of itself is rarely able to directly translate its violent activities into political effects commensurate with these stated goals. More often, terrorist actions create an effect that indirectly contributes to their political objective. Violence can be seen, in the perspective of the terrorist, as propaganda by deed, a concept that has roots in the nineteenth century. Alternatively, insurgency is a more direct strategic approach that links its political goals to a military operational plan. Conceptualised originally by Mao, and amended and ameliorated by subsequent generations of thinkers and practitioners of revolutionary war, insurgency is focused on a political objective which can be reached directly by offering an alternative political model: alternative governance for a population in a specific territory.[3]

Organisational differences take shape via the routes of recruitment and the structures of groups. Terrorists rely on secrecy, recruit on a small scale and are highly selective in this recruitment process. The survival of the group depends on the maintenance of secrecy and a guarded life in the underground, and less than careful selection runs the risk of detection and group demise. The small-scale organisational structure that these groups embrace falls short in cases where they manage to attract significant popular support. If the group fails to accommodate this support, it is bound to decline. This is where insurgents hold stronger cards. Their organisational structure is able to welcome recruits, in fact it actively seeks to welcome them. These individuals will build the support base on which the core structure of the group relies. The process of recruitment is less selective and therefore leads to a risk of denunciation of the insurgent group.

The social relations between the group and the wider population form a last distinctive feature of the two strategic approaches. For collective political violence to be effective and successful, popular support and legitimacy are necessary. Active or passive support for terrorist organisations is often more an 'aspiration by way of inspiration' than a clear tactical or operational goal.[4] For insurgents, without popular support they cannot exist. Human and material capabilities are necessary for the group to function and only the population, whose support they must foremost seek, can provide this.

These distinctive features have consequences for the counter-measures that can be employed. What works against a group that uses violence as a call to arms, is secretive and is small-scale is fundamentally different from what works against a group that aspires to gain control over a population by way of offering governance and a social contract. Both terrorist and insurgent strategies are characterised by extreme flexibility and adaptability. Non-state

---

Routledge Handbook of Insurgency and Counterinsurgency. London: Taylor & Francis.

4   Duyvesteyn and Mario Fumerton, 'Insurgency and Terrorism: Is there a difference?' p. 38.

---

3   Paul B. Rich and Isabelle Duyvesteyn. 2012. *The*

actor groups can shift between the strategies of terrorism and insurgency and have been known to do so in many instances. Over the course of their existence, the groups mentioned at the start of this contribution have embraced both insurgency and terrorism. The Shining Path in Peru put a Maoist insurgency strategy into practice that involved territorial control and alternative forms of governance. Since the apprehension of their leader, Abimael Guzman, in the early 1990s, the group has switched to a more terrorist approach. Hezbollah has interestingly moved from being a terrorist group, to an insurgency strategy focused on safeguarding the rights of the Shi'ite population in Lebanon, to becoming a full participant in the official politics of the Lebanese state. Al Qaeda and its many incarnations since its inception in the 1980s used the territory of the Afghan state to launch its worldwide struggle, employed a terrorist strategy, but according to many experts is now merely a network or even an ideology or inspiration.

Counter-terrorism and Substitution

The flexibility and adaptability of these violent non-state actors to shift between approaches lead to increased complexity for states attempting to counter them. These transformations are given shape prominently in a substitution or 'waterbed' effect. There are four forms of substitution: tactics, targets, territory and time – the T4 of substitution.[5] Terrorists shift between tactics; when one tactic becomes more difficult, they shift to other more easily executable tactics.[6] For example, airplane hijacking in the early 1970s was extremely popular

among terrorist groups. These hijackings were not intended to kill people but to attract attention and were highly effective. With the institution of safety measures such as metal detectors and luggage checks at airports, the practice almost disappeared but conventional bombings rose sharply. Furthermore, there is also evidence that non-state armed groups copy successful tactics from others. One example is the spread of suicide terrorism.

Similar to shifts in tactics, targeting is subject to frequent change. When targets become less accessible, a shift to others is commonly observable. An example here are the embassy fortifications that became standard practice after the embassy bombings in East Africa in 1998. The bombing of these diplomatic representations dwindled but targeting alternative American targets increased.

Substitution in the shape of territory is visible in spillover effects or conscious choices to carry out attacks in previously untouched areas. One example is Hezbollah, which has purportedly carried out attacks in Europe and South America in its struggle against Israel.

The last substitution effect is postponement in time. This is very difficult to prove. When did an organisation decide to wait until a later moment or more conducive period of time for its attacks? Still, it forms part of the range of options available to terrorist and insurgent groups.

The four forms of substitution and their examples point to the close links between substitution and counter-measures. A very strong cause and effect relationship is visible. Counter-measures affect choices of tactics, targets, territory and time and therefore form a prominent witness to their effect. This also shows that the resolution of one problem tends to create another. What are the consequences that deserve further attention?

5   Bruno S. Frey, 2004. *Dealing with Terrorism: Stick or Carrot?* London: Edward Elgar.

6   Walter Enders and Todd Sanders, 2000. "Is Transnational Terrorism Becoming More Threatening?; A Time-Series Investigation." *Journal of Conflict Resolution* 44 (3): 307-332. Walter Enders, 2004. "What do we Know about the Substitution Effect in Transnational Terrorism?" In Andrew Silke (ed.) *Research on Terrorism: Trends, Achievements & Failures*, London: Frank Cass, pp. 119-137.

Consequences for CT

These short reflections lead to several pressing issues. Counter-measures cause shifts in strategic approaches and substitution. What can work against groups working with a terrorist approach, however, is not the same as what can be effective against insurgents. On the basis of previous experiences, to counter-balance the attractiveness of insurgent claims the provision of a working social contract can be effective. The flip side of this argument has recently been observed in the areas under the control of Islamic State for example.[7] The alternative offer of a credible social contract in the absence of alternatives contributed to its hold over populations and territory. A Syrian and Iraqi state alternative was absent. However, countering terrorist groups by way of a viable counter-measure does not make much sense. A related issue here is whether the distinction between terrorism and insurgency does not in fact denote a distinction between the Western and non-Western world. It is a fact that territory cannot easily be contested against a well-functioning Westphalian state and it would require significant capability. Does this make insurgency exclusively a problem of the developing world and does it rule out strategic terrorism? Some more scholarly attention investigating this would be welcome.

Second, if terrorism is a problem of the Western world with little or no chance of rival territorial control, except possibly for foreign sanctuary, how can we think of counter- measures? Where do the weaknesses lie in the approach of terrorism? The organisational structure can be targeted and the violent activities curbed, but again such groups are highly adaptable. The political challenge that terrorism poses is where exploitable weaknesses potentially reside.

When counter-terrorism measures feed substitution behaviour, the valid question is that of the extent to which we have shifted the problem rather than resolved it. Different tactics, other targets or a shift in territory have morphed the challenge posed by these violent groups. What then is our definition of success? Is a shift a form of success? These questions require some sort of answer if we are to break the cycle of measure and counter-measure repeating itself over and over again.

....

7   Craig Whiteside, 2016. 'The Islamic State and the Return of Revolutionary Warfare.' *Small Wars and Insurgencies* 27 (5), pp. 743-776.

THE NEW CRIME-TERROR NEXUS IN EUROPE

Rajan Basra[a] & Peter R. Neumann[b]

Research Fellow at the International Centre for the Study of Radicalisation

Professor of Security Studies, King's College London & Director, International Centre for the Study of Radicalisation

Introduction

Throughout Europe, there is a merging of criminal and extremist *milieus*. German Federal Police state that of the 778 German foreign fighters about whom they have sufficient information, two-thirds had police records prior to travelling to Syria.[1] The Belgian Federal Prosecutor says that approximately half of the country's jihadists had criminal records prior to leaving for Syria.[2] A United Nations report suggests a similar pattern amongst French foreign fighters.[3] Officials from Norway and the Netherlands told us that "at least 60 per cent" of their countries' jihadists had previously been involved in crime.[4] It is for this reason that Alain Grignard, the head of Brussels Federal Police, described Islamic State as "a sort of super-gang."[5]

This article describes the dynamics of this crime-terror nexus in order to understand what it means for the terrorist threat and how to counter it. The article addresses four questions. How does criminality facilitate radicalisation and recruitment? What is the role of prisons? Do criminals possess skills that make them more effective as terrorists? And how do criminals finance their terrorist activities?

To analyse these issues, a multi-lingual team of ICSR researchers compiled a database containing the profiles of 79 recent European jihadists with criminal pasts. As far as we know, it is the first database of its kind. While it is not a representative survey of European 'gangster' jihadists, it has provided source material for a better understanding of the different dynamics and developments. By analysing the pathways, motivations and actions of these jihadists, we have been able to ascertain some characteristics that define the crime-terror nexus in the context of the current jihadist threat.

In the following sections, we will examine two themes for which we have found evidence in our database: (1) radicalisation, including the prison environment; and (2) 'skill transfers,' including criminal financing.

What we observe in the case of jihadist recruits in Europe is not a convergence of criminals and terrorists as organisations but of their social networks, environments or *milieus*. In other words: rather than being one or the other, criminal and terrorist groups have come to recruit from the same pool of people, creating (often unintended) synergies and overlaps that have consequences in terms of how individuals radicalise and operate. This is what we call the new crime-terror nexus.

1   BKA, BfV & HKE (2016), 'Analyse der Radikalisierungshintergründe und -verläufe der Personen, die aus islamistischer Motivation aus Deutschland in Richtung Syrien oder Irak ausgereist sind – Fortschreibung 2016', p.18.

2   Christophe Lamfalussy (2015), 'Un djihadiste belge sur deux a un passé de délinquant,' *La Libre*, 14 August.

3   United Nations Analytical Support and Sanctions Monitoring Team (2015), 'Analysis and recommendations with regard to the global threat from foreign terrorist fighters', p.11.

4   Interviews with Dutch and Norwegian police officers (2016), 1-2 September.

5   Paul Cruickshank (2015), 'A view from the CT foxhole: an interview with Alain Grignard, Brussels Federal Police', *CTC Sentinel*, 21 August.

Radicalisation and Recruitment

With criminal pasts being prominent among both foreign fighters and the perpetrators of the recent 'wave' of terrorist attacks, one of the most compelling questions is how criminal pasts contribute to processes of radicalisation.[6] The profiles and pathways that emerge from our database suggest that the jihadist narrative is surprisingly well-aligned with the personal needs and desires of criminals: it can offer 'redemption' while also licensing criminality. These processes can take place within prisons, which are likely to become important centres of gravity for jihadism in the coming years.

The Redemption Narrative

Recurrent among criminals in our database was what we term the 'redemption narrative.' These were criminals who had experienced what Quintan Wiktorowicz calls a "cognitive opening," a shocking event or personal crisis that prompted them to re-assess their lives and become open to a radical change of values and behaviour.[7] They realised a need to break with their criminal past and make up for their 'sins.' This then provided the rationale for their turn to religion and justified their involvement with jihadist groups.

That they sought redemption in jihadism instead of other more mainstream forms of religion or spirituality may be explained by a strong alignment of needs and narratives. In other words, involvement in jihadism offered redemption from

crime while satisfying the same personal needs and desires that had led them to become involved in it. Just like the criminal gangs of which they used to be members, jihadist groups offer experiences of power, violence and adventure, and provide their members with a strong identity and a sense of rebellion and being anti-establishment. This made the 'jump' from criminality to terrorism smaller than is commonly perceived – especially when considering that, unlike al-Qaeda, Islamic State requires practically no religious knowledge or learning, and – at least in the recruitment phase – cares less about the complexities of theological discourse. For a criminal with a guilty conscience, the jihadism of Islamic State could seem like a perfect fit.

Among the most prominent examples is Abderrozak 'Big A' Benarabe, a long-time criminal from Copenhagen who turned to jihadism after his brother was diagnosed with cancer. When explaining why he became a foreign fighter, he immediately referred to his criminal past: "… some people have died at my hands. This is a big problem when I meet Allah … It's not good enough just to pray with all the shit I've done."[8]

Legitimising Crime

While the jihadist narrative can be a source of redemption, it may also serve to legitimate crime. This is nothing new. Anwar al-Awlaki, the influential radical cleric, repeatedly told his followers that "stealing from your enemies" in the *dar al-harb* (lands of war) is permitted, and in certain cases obligatory.[9] This has the potential to be enormously effective because it offers criminals an opportunity for 'redemption' without requiring any change of behaviour. Islamic State shares this doctrine, stating in its Rumiyah magazine that

---

6   In this context, radicalisation refers to the personal circumstances, experiences, narratives, networks and other factors that explain an individual's involvement in extremism and their mobilisation to engage in violence. For more, see Peter R. Neumann (2013), 'The Trouble with Radicalization,' *International Affairs,* Vol 89, No 4, pp. 873-93.

7   Quintan Wiktorowicz (2005), *Radical Islam Rising: Muslim Extremism in the West* (London: Rowman & Littlefield), p.20.

8   Nagieb Khaja (2014), 'On the frontline in Syria: The Danish gangster who turned jihadi,' *The Guardian*, 7 July.

9   Al-Awlaki cited in Thomas Joscelyn (2011), 'Anwar al Awlaki: Jihadists should steal from disbelievers,' *Long War Journal,* 17 January.

"the kafir's wealth is halal for you, so take it."[10] Far from considering such offenses a sin, some jihadists actively encourage crime.

The most prominent example is the network around Khalid Zerkani. Born in Morocco in 1973, Zerkani moved to Belgium as an adult. Whilst he had engaged in petty crime and shoplifting, his greatest talent was as an Islamic State recruiter. He encouraged young men, mostly with Moroccan backgrounds, to commit petty crimes and robberies in Brussels.[11] This was justified on religious grounds: as a witness in his trial testified, Zerkani reassured recruits that "to steal from the infidels is permitted by Allah."[12]

Prior to his 2014 arrest, Zerkani had become a hugely influential figure in the Brussels jihadist scene, responsible for the mobilisation of up to 72 foreign fighters.[13] His most infamous protégé was Abdelhamid Abaaoud, a key coordinator of the network that carried out the mass-casualty attacks in Paris in November 2015 and Brussels in March 2016. More than any other example, the way he operated illustrates the idea behind the new crime-terror nexus, because it produced a near-perfect merging of the two *milieus*.

Prisons

One place where these *milieus* naturally meet is prison. Prisons have been in the spotlight for nearly a decade as places where radicalisation occurs.[14] 57 percent (45 out of 79 profiles) of our sample spent time incarcerated prior to their mobilisation, with sentences ranging from one month to over ten years. More significantly, at least 31 percent of those who spent time in prison (14 out of 45 profiles) radicalised there, although – in most cases – the process continued and intensified after their release.

This is because prisons are places of vulnerability. For many new inmates, the very fact of imprisonment is a personal crisis which raises profound questions about their lives while offering ample time to search for meaning. While cut off from their immediate family, friends and wider society, inmates find themselves in an environment which is often hostile, unfamiliar and tribal in nature, with divisions along religious or ethnic lines. New inmates are mentally and physically vulnerable, and may experience 'cognitive openings' – a willingness and desire to identify with new ideas, beliefs and social groups.[15]

For the same reason, jihadist recruiters view prisons as places of opportunity. Not only are inmates vulnerable and they experience cognitive openings, thereby making them receptive to jihadist ideas, but they also tend to be part of the demographic that jihadist groups are keen to attract: young men from Muslim backgrounds (but rarely practicing) who are impulsive and willing to take risks, and have already been in conflict with established authorities.[16] Far from being an obstacle, their criminal pasts have desensitised them to law-breaking and violence, and may, in fact, have provided them with useful skills for a terrorist career. From the jihadists' perspective, prisons are the perfect 'breeding ground.'

10   Islamic State (2017), Rumiyah issue 9, p.12. See also Rumiyah issue 11 for more encouragement of criminal behaviour.

11   Patrick J. McDonnell (2016), '"Papa Noel" – the militant recruiter in Brussels who groomed young men for violence,' *Los Angeles Times*, 28 March.

12   Andrew Higgins and Kimiko De Freytas-Tamura (2016), 'A Brussels Mentor Who Taught "Gangster Islam" to the Young and Angry,' *New York Times*, 11 April.

13   Pieter Van Ostaeyen and Guy Van Vlierden (2016), 'Belgian Fighters in Syria and Iraq – An Important Review of Our Data' 3 August, available at: https://pietervanostaeyen.com/2016/08/03/belgian-fighters-in-syria-and-iraq-an-important-review-of-our-data/ (last accessed 22 July 2017).

14   See Peter R. Neumann (2010), 'Prisons and Terrorism: Radicalisation and De-radicalisation in 15 Countries,' *The International Centre for the Study of Radicalisation (ICSR)*.

15   Ibid., p.26.

16   See Andrew Silke (2008), 'Holy Warriors: exploring the psychological processes of jihadi radicalization,' *European Journal of Criminology*, Vol 5, No 1, p. 107.

Even those *outside* of prison can exploit this, as shown by the prison outreach of Shiraz Tariq, leader of the Danish Salafist group *Kaldet til Islam* (Call to Islam).[17] He wrote letters to imprisoned members of gangs in Copenhagen, appealing to their guilty consciences. The group's Facebook page stated that Muslims in prisons "[are] getting off track, so we thought we could write letters to [them] and remind them of Allah. They have plenty of time to read."[18] While it remains unknown how effective this was – the group also saw *non-prison* recruits travel to Syria – it is an example of an attempt to recruit criminals.

Given the recent surge in terrorism-related arrests and convictions, and the rapidly expanding number of convicted terrorists in custody, prisons are likely to become more significant as centres of gravity for the jihadist movement.

Skill Transfers

One of the most disturbing aspects of the new crime-terror nexus is the potential for criminal 'skills' to be transferred to terrorists. Our database illustrates four factors: first, that individuals with a criminal past tend to have easier access to weapons; second, that many are adept at staying 'under the radar' and are familiar with evading the authorities; third, that their experience and familiarity with violence lowers their (psychological) threshold for involvement in terrorist acts; and fourth, that crime is often used to fund terrorism.

Weapons

As early as 2013, the Danish intelligence service warned that the strong presence of criminals amongst Danish jihadists would lead to a proliferation of firearms among them.[19] Two years later, the warning came true when Omar el-Hussein carried out two shootings in February 2015. Between the two attacks, he went to his neighbourhood of Mjølnerparken and gave the M95 rifle that he had used during the first shooting to a former fellow gang member for him to dispose of it.[20] This rifle was itself stolen during a robbery in 2013.[21] He also met with former gang associates, one of whom was in possession of the same ammunition that el-Hussein used in the second attack, making it plausible that he had supplied him with new ammunition. In short, his gang connections eased his access to weapons.

Islamic State itself has acknowledged the value of their operatives appearing like "ordinary" criminals. In the July 2015 issue of *Dar al-Islam*, their French language magazine, the group advised operatives to conceal all external displays of religiosity when acquiring weapons, and instead, adopt the look of a "*jeune de cité*" (a youth from the town) who is "looking to make a robbery with a weapon."[22] This advice proved to be unnecessary, as many of their supporters genuinely fit this profile.

Staying 'Under the Radar'

In addition to procuring firearms, access to criminal networks makes it easier for terrorists to 'stay under the radar'. This includes, for example, the use of fake documents and access to safe houses which enable terrorists to evade the authorities, and therefore increases the likelihood of a plot turning into a successful attack.

---

17   Tariq himself did not have a criminal record, although many in *Kaldet til Islam* did; they were included in the research sample.

18   Simon Bedtsen, Mette Dahlgaard and Kasper Krogh (2013), 'Fængslede muslimer skal have brev fra ekstreme islamister', *Berlingske*, 2 October.

19   PET Center for Terroranalyse (2015), 'Truslen mod Danmark fra personer udrejst til Syrien', 23 October, p.3.

20   Niels Vedersø Østergaard (2016), 'Terrortiltalt hjalp Omar El-Hussein,' *Berlingske*, 17 March.

21   Michala Rask Mikkelsen (2015), 'Riffel fra terrorangreb blev stjålet under hjemmerøveri', *Berlingske*, 18 February. The rifle model is otherwise known as an RK 95 TP.

22   Al-Hayat (2015), 'Dar al-Islam Numéro 5,' p.33.

The Paris and Brussels network that carried out attacks in November 2015 and March 2016 did exactly this. Their use of fraudulent identities allowed the network to wire money, travel between countries, rent cars and – crucially – acquire safe houses.[23] For example, Khalid el-Bakraoui used forged identification papers – adopting the name 'Ibrahim Maaroufi' – to rent an apartment in Charleroi which was subsequently used by at least two of the Paris attackers.[24] Another apartment in Schaerbeek – rented under the pseudonym Fernando Castillo – was used as a bomb factory to manufacture the TATP explosives and suicide vests used in the Paris attacks.[25]

Rather than becoming forgers themselves, the terrorists who launched the attacks in Paris and Brussels used their contacts in the criminal *milieu* to reach out to forgers who serviced people traffickers. This is how they came across Djamal Eddine Ouali, an Algerian who ran a forgery operation in Brussels. The supposed 'profit vs. ideology' dichotomy, which is debated in the academic literature,[26] was no barrier in this case. There is no evidence that Ouali knew of their true intentions, or was even interested in them. Instead, they probably appeared as 'ordinary' customers from a criminal *milieu*. As the Belgian investigator in charge of Ouali's case said, "[He] was a professional document falsifier whose main goal was to make as much money as possible from his business."[27]

23   Lori Hinnant (2015), 'Piecing together Salah Abdeslam's itinerary in Paris attacks: Days on end at the wheel and months of planning', *Associated Press*, 10 December.

24   The New York Times staff (2016), 'Ibrahim and Khalid el-Bakraoui: From Bank Robbers to Brussels Bombers,' *The New York Times*, 24 March.

25   Michael Wolgelenter (2016), 'ISIS Militant Returned to Belgium Before Paris Attacks, ' *New York Times*, 13 January.

26   Santiago Ballina (2011), 'The-Crime Terror Continuum Revisited," *Journal for Policing, Intelligence and the Power of Informal Networks*', Vol 6, No 2, 2011, pp.121-124.

27   Maïa de la Baume and Giulia Paravicini (2016), 'Inside

Familiarity with Violence

These practical and logistical skills are supplemented by a more intangible 'skill': that of familiarity with violence. 65 percent of the individuals in our database had been involved in violent crime. Among the 30 individuals who were involved in plots, this figure rose to 80 per cent. Routine engagement in violence as a criminal may lower the (psychological) threshold for becoming involved in violence as a terrorist. Our database shows that the period of mobilisation among the 30 individuals involved in domestic plotting was often extraordinarily short, often less than four months or even just a few weeks. These findings support the idea that previous criminality produces more volatile terrorists.

The case of Mohammed Merah – who killed 7 people, including three Jewish children, near his hometown of Toulouse in March 2012 – illustrates the often extreme histories of violence found. His attacks were the culmination of a life story characterised by routine violence, involving two stays in prison and 18 convictions for assaults, robberies, and thefts.[28] As a teenager, Merah was reported at least 15 times for acts of violence, and was described as having "a violent profile from childhood and behavioural troubles."[29] This would continue into adulthood: in 2006 after his uncle asked him to stop making a noise with his quad bike, Merah beat him in the face with a fire extinguisher.[30] In 2010 he blinded a teenage girl during an assault.[31] By the time Merah travelled for terrorist training in Waziristan in 2011, no one

the Brussels flat where terrorists scored fake IDs,' *Politico*, 31 March.

28   Alex Jordanov (2015), 'Mohamed Merah, de cas social à idole du jihad', *Les Inrocks*, 17 June; and Virginie Andre and Shandon Harris-Hogan (2013), 'Mohamed Merah: from petty criminal to neojihadist', *Politics, Religion & Ideology*, Vol 14, Issue 2, pp.307-319.

29   BBC (2012), 'Obituary: Toulouse gunman Mohamed Merah', *BBC News*, 22 March.

30   Alex Jordanov (2015).

31   John Rosenthal (2016), 'Merah: The 'Untold Story' of a French Jihadist Icon', *World Affairs*, Winter.

Financing

It is no surprise that criminal pasts also enable terrorist financing. Solid empirical examinations of this phenomenon are surprisingly rare, although two recent studies have started cataloguing the funding of jihadist activities in Europe. A report by Magnus Normark and Magnus Ranstorp focuses on how European foreign fighters funded their travels to Syria. In addition to loans, private donations, bank fraud and business fraud, they consistently emphasise the role of petty crime.[32] A study by Emilie Oftedal examines the financing of 40 jihadist plots between 1994 and 2013: although nearly three-quarters generated at least some of their income from legal sources, she shows that criminality played a significant role, with nearly 40 percent of the plots drawing on the proceeds of crime.[33]

Our database suggests that jihadists continue to do what they are familiar with, and so their criminal fundraising merely involves a change of *purpose* rather than a change of *behaviour*. The perpetrators of the January 2015 Paris attacks showed this. Saïd Kouachi, for example, sold counterfeit goods and received money from Al-Qaeda in the Arabian Peninsula. Not all of this money went into funding the Charlie Hebdo attack, but some of it did.[34] How is it possible to distinguish one from the other? Amedy Coulibaly, on the other hand, was selling drugs only a month before the attacks, in addition to being owed street debts worth €30,000.[35]

Coulibaly did not need to change his criminal fundraising tactics. In these cases, the common thread was not any particular source of funding (be it counterfeits, drugs or cash) but personal continuity. Therefore, it can be difficult to separate funds raised for terrorism from money spent on other, often entirely mundane, purposes.[36]

Conclusion

The convergence of criminal and terrorist *milieus* – what we call the new crime-terror nexus – is real, and has profound implications for how jihadist groups in Europe operate. For the first time, there is near-complete alignment between a group like Islamic State and criminals attracted by its core counter-cultural message of redemption through strength, power and violence. Islamic State and/or its successors increasingly find recruits in European 'ghettos,' in prisons, among the European 'underclasses' and those who have previously engaged in violence and illegal acts. Thus, those who are becoming part of the jihadist counter-culture can apply their criminal skills to terrorist purposes. Indeed, many individuals continue their involvement in crime whilst radicalising.

Countering terrorism, therefore, needs to address this social aspect of the problem. However, more attention also needs to be paid to prisons and to countering 'petty' and organised crime (as well as the people engaging in it). Institutional silos – for example, the separation between countering crime and countering terrorism, or between counter-terrorism and 'criminal' police – need to be broken down. There may also be a case for more collaboration between security agencies and local authorities, and also the private sector, for example in public-private partnerships.

32   Magnus Normark and Magnus Ranstorp (2015), 'Understanding terrorist finance: Modus operandi and national CTF regimes', *Swedish Defence University*, 18 December.

33   Emilie Oftedal (2015), 'The financing of jihadi terrorist cells in Europe,' *FFI Report, Norwegian Defence Research Establishment*, p.3, p.19, and p.26.

34   Katrin Bennhold and Eric Schmitt (2015), 'Gaps in France's Surveillance Are Clear; Solutions Aren't,' *New York Times*, 17 February.

35   BBC (2015), 'Paris attacks: Investigators turn up new leads,' *BBC News*, 19 January; and L'Obs, 2015, 'J-12 jours avant "Charlie" et l'Hyper Cacher: récit d'un effroyable compte à rebours', *L'Obs*, 24 February.

36   Peter R. Neumann (2017), 'Don't Follow The Money: The Problem With the War on Terrorist Financing,' *Foreign Affairs*, July/August issue.

Not least, many assumptions about radicalisation need to be reconsidered, e.g. that a pious person is not likely to also be a criminal or that someone 'acting like a gangster' cannot possibly be also involved in terrorism. With criminal and terrorism *milieus* merging, the fight against crime has become – to a significant extent – a national security issue.

JIHADIST STRATEGIES ON THE INTERNET: HOW THE DECLINE IN IS OFFICIAL PROPAGANDA RAISES THE VISIBILITY OF PRO-IS USER-GENERATED CONTENT

Antonis Samouris

Academic affiliation: Leiden University, Institute of Security and Global Affairs, Wijnhaven Building, Turfmarkt 99, 2511 DP, The Hague, Netherlands

In a relatively short period of time – three years – the so-called Islamic State (IS) terrorist organisation has managed to revolutionise jihadist propaganda online. Because of its sheer volume, penetrating messages and strategic exploitation of the internet and social media vulnerabilities, IS media content in the virtual space is expected to survive any contraction of the organisation on the ground. The aim of this paper is to shed light on how IS adapts its communication strategy on the internet in order to expand its virtual presence in the face of territorial loss. This involves the employment of market promotion techniques and taking advantage of the user generated content (UGC) that IS sympathisers produce on social media. A core argument of the paper is that containment of the IS presence online depends on a deeper understanding of IS communication strategies on the internet so that a public-private response can be designed.

Since the announcement of the caliphate in mid-2014, IS has followed an aggressive social media campaign aiming to magnify the impact of military victories in Syria and Iraq and to bring wider audiences to support its cause. Compared to al-Qaeda's (AQ) use of the internet for propaganda purposes, IS's approach of publicising its atrocities against captives and openly threatening non-affiliated jihadist groups, including AQ itself, at first sight appeared risky and potentially counter-productive. Nevertheless, the organisation's traction on social media demonstrates that the IS communication strategists have understood how digital technology and especially the proliferation of mobile devices have changed the structure of communication from a hierarchical system, in which terrorist organisations disseminated their messages to followers through tightly controlled internet forums, to a horizontal structure, in which the spread of the message is based on peer-to-peer dissemination.[1] In fact, it is through a seemingly decentralised network of media operatives on social media that IS ensures its message gets across to social media users and resonates with its targeted audiences.

It is worth noting that the first generation of AQ militants were reluctant to use the internet in their communications or to disseminate the organisation's propaganda. Usama bin Laden's preferred practice was to use couriers to deliver his pre-recorded audio or video messages to media outlets with global outreach for their broadcast.[2] Furthermore, the first dedicated jihadist discussion forums were created as late as 2003.[3] These forums were publicly advertised by supporters, after AQ-affiliated static websites had

---

1   For a detailed analysis of the impact of digital technology on IS strategic communications, see The Nato Strategic Communications Centre of Excellence (2017), Strategic Communications: Insights from the commercial sector, http://www.stratcomcoe.org/strategic-communications-insights-commercial-sector

2   "Al-Jazeera: Bin Laden tape obtained in Pakistan," NBC news, 30/10/2004 http://www.nbcnews.com/id/6363306/ns/us_news-security/t/al-jazeera-bin-laden-tape-obtained-pakistan/#.WXx_9ekUmUk

3   Anne Stenersen, "The history of the jihadi forums", Jihadica.com, 04/03/2009 www.jihadica.com/the-history-of-the-jihadi-forums

repeatedly been taken down.[4] With time, however, jihadist organisations realised the importance of the internet to their effort to develop their strategic communications model. Media operatives on the internet became responsible for polishing the brand of the organisation, spreading its message to followers and sympathisers and carrying out the digital jihad against the organisation's detractors online. In fact, the 'media mujahid' was granted equal status to the mujahid who fights the jihad on the physical battlefield.[5]

Nonetheless, this system was based on a series of rigid checks and balances. Until late 2012, much of the 'media jihad' was conducted in internet jihadist forums that performed, among other things, the function of content authenticator on the latest propaganda releases. In addition, the administrators of the forums were responsible for editing out any cacophony coming from disenchanted followers in order to safeguard the consistency of the jihadist message. However, in early 2013 a significant shift of jihadist activity from forums to social media such as Twitter and Facebook took place.[6] This tendency was further intensified, resulting in a rapid degradation of jihadist forums by the end of 2014.[7] Beside structural problems, such as limited outreach to the public, a constant fear of infiltration and the resulting suspicion[8] and dissatisfaction of some

members, a major reason behind this development was the falling-out between AQ and ISIL[9] after the latter's rejection of al-Zawahiri's admonishment to leave the leading role in the Syrian jihadist opposition to Jabhat al-Nusra.[10]

An assertive IS after the fall of Mosul, and in particular the announcement of the caliphate in mid-2014, encountered no constraints on the use of social media to project its totalitarian plan for the region. Its communication strategy was based on the following elements: a multi-layered message targeting a variety of audiences from IS members to sympathisers, to Sunni Muslims in general, to enemies (including those Muslims who did not accept IS's claim to Muslim leadership); a massive production of high-quality movie-style propaganda; an apparent decentralization; and the use of popular social media platforms, such as Twitter, Facebook, YouTube and Google services, for the dissemination of its products. In this early phase, Twitter appears to have played an instrumental role in the conveyance of the IS online strategy. The popularity and speed of message delivery of this social media platform ensured that the IS message was rapidly delivered to large audiences of sympathisers, enemies and unconcerned users.[11] On release, each new IS propaganda item is circulated by a large pool of core disseminators (IS media operatives) using dedicated hashtags to create the necessary traction before reaching the larger Twitter network. The tweets include links to other social media, such as YouTube and Facebook, where the content can be accessed and downloaded.[12] Quick and agile movement among social media platforms

4   Awan, Akil N. and al-Lami, Mina (2009) "Al-Qa'ida's virtual crisis," *The RUSI Journal*, 154:1, pp. 56-64.

5   Ranstorp, Magnus and Normak, Magnus eds. (2015) Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond, Routledge, pp. 118-119.

6   Bunzel, Cole, (2013) Are the Jihadi Forums Flagging? An Ideologue's Lament www.jihadica.com/are-the-jihadi-forums-flagging-an-ideologue's-lament/

7   Weimann, Gunnar (2017) "Squirting venom on Twitter," paper presented at the TASM Conference at Swansea University in June 2017.

8   Hegghammer, Thomas (2014) "Interpersonal trust on jihadi Internet forums," draft chapter to be included in Diego Gambetta (ed.), Fight, Flight, Mimic: Identity Signalling in Armed Conflicts, forthcoming, available at http://hegghammer.com/_files/Interpersonal_trust.pdf

9   "Islamic State in Iraq and the Levant" was the predecessor organisation to "Islamic State".

10   Weimann, G. (2017)

11   According to Stratcom research, "The speed at which messages can be delivered in the contemporary information environment is at least as important as their content. The first message delivered in audience dialogue is the loudest and sets the pace in controlling the subsequent debate," p. 18.

12   Weimann, G. (2017)

enhances the resilience of the jihadist online network against any disruptive attempt. In fact, the IS dispersed network of social media accounts has been described as a "swarmcast which constantly reconfigures much like the way a swarm of bees or flock of birds constantly reorganises in mid-flight [allowing for] the persistent presence of jihadist content online."[13]

In parallel, IS employs marketing techniques to promote its products online. High-profile propaganda items, such as major video productions, are announced with teasers in a "coming soon" phase that can last one to two days before the actual release of the item. This maximises followers' anticipation and attracts the attention of other users. The launch of new propaganda items is accompanied by aggressive dissemination tactics on Twitter through the activation of dormant accounts, bots and the use of dedicated hashtags or hijacked hashtags advertising popular events.[14] Outlinks embedded in the tweets point to the content in other social media, such as streaming platforms and file-sharing sites, magnifying the impact of the dissemination of the new item. The last part of this three-phase strategy consists of re-cycling the material online at intervals through re-uploads, by advertising new links and by making references to it in new propaganda productions.

Initially, a slow and uncoordinated reaction to terrorist abuse of social media granted IS media operatives the necessary room to extend their influence, making IS propaganda noticeable across the spectrum of social media users and attracting new followers.[15] The more committed

among them probably spend hours online to further spread IS propaganda and also themselves generate and circulate material in support of the terrorist organisation. These new jihadist 'prosumers' on social media have been labelled 'ISIS fanboys' because they combine their pledge to join the fight against the enemies of IS in the virtual domain with their fascination with geek culture.[16] Thus, official IS propaganda seems to be circulated by core disseminators first before being further disseminated by IS fanboys, often accompanied with their own UGC.

Towards the end of 2015, and especially in the aftermath of the 13 November attacks in Paris, drastic action undertaken jointly by governmental organisations, civil society and social media companies resulted in the disruption of much of IS activity on at least some of the major social media platforms.[17] This forced the IS media operatives to move to less hostile social media to implement their communication strategy.[18] In fact, throughout 2016, Telegram became increasingly the platform of choice for the IS online community as it allowed for a relatively free space in which the preparation of jihadist media campaigns (*ghazawat i'lamiyya*) could

13   Fisher, Ali (2015) Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence, Perspectives on Terrorism, vol. 9, no. 3 http://www.terrorismanalysts.com/pt/index.php/pot/article/view/426/html

14   Milmo, Cahal (2014) "Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter," http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-9555167.html

15   In Autumn 2014, various studies calculated the number

of pro-IS accounts on Twitter as being in the area 45,000-70,000. For example, see Berger, J.M. and Morgan, Jonathon (2015) "The ISIS Twitter Census," Brookings Analysis paper no. 20 https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf and Statista (2014) "Twitter presence of ISIS as of Fall 2014," https://www.statista.com/statistics/412435/isis-twitter-accounts-tweets/

16   Frenkel, Sheera (2014) "Meet The "ISIS Fanboys Spreading The Message Of Iraq's Most Feared Terror Group", https://www.buzzfeed.com/sheerafrenkel/meet-the-isis-fanboys-spreading-the-message-of-iraqs-most-fe?utm_term=.wxjwn5OQe#.wgzxog0P9

17   Europol "Terrorism Situation and Trend Report 2016," pp. 16-17. https://www.europol.europa.eu/sites/default/files/documents/europol_tesat_2016.pdf, Yadron, Danny (2016) Twitter deletes 125,000 Isis accounts and expands anti-terror teams, https://www.theguardian.com/technology/2016/feb/05/twitter-deletes-isis-accounts-terrorism-online

18   Europol "Terrorism Situation and Trend Report 2017," p. 29 https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017

be initiated.[19] To this end, IS core disseminators, having privileged access to new content, prepare the ground for upcoming propaganda releases by simultaneously posting announcements, banners and teasers in 'mirror channels' on Telegram.[20] This signals to the community of IS sympathisers on Telegram that a time for coordinated action is approaching, meaning the aggressive promotion of new content across social media. Since Telegram is a closed environment which is not indexed by search engines, and its content cannot be accessed by the general public unless they join the pro-IS channels, it is the role of both core disseminators and IS sympathisers on Telegram to advertise new content on more accessible social media platforms. The IS fanboys activate a vast network of dormant accounts and bots, upload the content to file-sharing sites and streaming platforms and share the links with the public in a very short time after the release of the new propaganda item.[21]

What needs to be noted in this process is the authentication of IS products. As mentioned, official IS propaganda is first advertised and circulated by the core disseminators, who have privileged access to new content as they are part of the IS propaganda apparatus. Authenticity is validated through the simultaneous appearance of new content on the core disseminators' Telegram 'mirror channels.' This simple but rigorous system of validation eliminates any disinformation attempt by outsiders, as was shown by a failed attempt to plant fake RUMIYAH issues in the circulation model of IS official content. Monthly RUMIYAH, the flagship IS magazine addressing audiences in

eleven languages other than Arabic, is by its nature one of the core instruments of IS propaganda. For several issues between no. 3 (November 2016) and no. 10 (June 2017), the release of the original IS product was preceded a few hours earlier by fake versions of RUMIYAH uploaded on seemingly pro-IS channels on Telegram in an apparent effort to confuse supporters or collect information on them through malware embedded in the pdf file.[22] Despite the fact that the fake RUMIYAH issues were the result of a sophisticated effort to replicate the original production, their circulation on Telegram and Twitter did not take off as they were not supported by the core disseminators' channels.[23] Consequently, the fake issues were not picked up by the community of IS fanboys either, putting a swift end to the attempted disinformation campaign.

The above observation is connected with the outreach of IS's propaganda to audiences at present. The production and dissemination of official IS propaganda continues to be centrally orchestrated and not outsourced to IS fanboys. Nevertheless, after reaching its peak in mid-2015 propaganda production has been in steady decline ever since.[24] This can be considered to be largely the result of the targeted killing of a number of central figures

19   Prucha, Nico (2016) "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram," Perspectives on Terrorism, Vol. 10, No 6 http://www.terrorismanalysts.com/pt/index.php/pot/article/view/556/html

20   For more information on IS mirror channels on Telegram, see Smith, Laura (2017), Messaging app Telegram centrepiece of IS social media strategy http://www.bbc.com/news/technology-39743252

21   Europol "Terrorism Situation and Trend Report 2017," p.   29   https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017

22   Khayat, M. (2017) Release Of Two Suspicious Fifth Issues Of ISIS's 'Rumiyah' Magazine – Timeline, Characteristics, And Takeaways, MEMRI https://www.memri.org/jttm/release-two-suspicious-fifth-issues-isiss-rumiyah-magazine-–-timeline-characteristics-and

23   Fake Rumiyah no. 5 included fully-fledged articles with themes that closely resembled those in previous original Rumiyah issues. Fake Rumiyah no. 7 contained the exact titles of articles that later appeared in the original copy of the same issue, betraying an insider as the party behind the disinformation campaign.

24   West Point's CTC observed that the number of new propaganda visual releases dropped from 700 unique items per month in August 2015 to less than 200 items in August 2016. This figure must have dropped to half by mid-2017. What is worth noting is the fact that most of these items are short unedited videos from the battlefield and photo reports. Instead, high profile video production in 2017 is in free fall. See also MIton, Daniel (2016), Communication Breakdown: Unravelling the Islamic State's Media Efforts, CTC West Point https://ctc.usma.edu/v2/wp-content/uploads/2016/10/ISMedia_Online.pdf

in the IS propaganda machinery by coalition forces. It has put the terrorist organisation's media department under severe pressure.[25] In the face of a significantly lower volume of IS official propaganda, what is gaining in visibility is UGC produced by IS fanboys. Running their own Telegram channels, they react individually to major events (i.e. in the aftermath of terrorist attacks), producing content such as memes and banners that glorifies IS acts. Occasionally IS fanboys' UGC threatens new attacks, identifies targets and incites 'lone actors' to continue with the terrorist plotting. Normally, this type of UGC does not make it to the mainstream social media but remains within the confines of the fanboys' channels that post it. The reason is that UGC is not picked up by IS's core disseminators to enter the dissemination process. The multiplicity of fanboys' channels and the usual suspicion of infiltration attempts deter the IS propaganda machinery from appropriating any such content as official material. Nonetheless, the heightened alert about the IS threat is quite often leading IS propaganda observers[26] to bring to the surface the fanboys' UGC, confusing it or mixing it up with official IS propaganda. In several cases, reports based on UGC have hit the traditional media headlines, contributing to a climate of public fear and insecurity. Therefore, it appears that anti-IS actors can be responsible for bringing terrorist threats that do not come from the terrorist organisation itself to public attention, inadvertently playing the game of the IS propagandists.

Acknowledging this development can help the devising of better strategies for the containment of IS propaganda online. Although the massive production of high-quality IS propaganda in recent years will help the terrorist organisation to maintain a significant online presence in the future, its impact of radicalising individuals can be mitigated by restricting public access to it. First, because the IS propaganda apparatus is centrally controlled and dissemination centrally orchestrated, further loss in terms of infrastructure and territory is expected to have an increasingly adverse impact on new propaganda production. Targeting the core disseminators in social media can also impact its circulation mechanism. Second, private-public synergies can widen the range of actors engaging in the disruption of terrorist propaganda. Government agencies and larger social media companies can share their experiences in the field with smaller, in terms of resources, companies and civil society, forging a common front against terrorist abuse of the internet. Finally, better assessment of UGC as opposed to IS official terrorist propaganda and putting limitations on the publicising of it would further curb the terrorist organisation's outreach to online audiences.

Conclusions

IS strategic communications online have undergone a fundamental change. A recent loss of media infrastructure and resources has considerably curtailed the terrorist organisation's capabilities to produce new high-quality propaganda. Its dissemination model online is also facing significant challenges as social media companies and government organisations intensify their disruptive efforts. The combination of the above factors leads to attention to UGC produced by IS fanboys as a substitute for official IS content. Nonetheless, a clear separation between IS official propaganda and UGC is needed in order to conduct a more accurate assessment of the terrorist threat online. Based on that, public authorities, civil society and private parties can build tailored measures aiming to disintegrate IS's online strategic communications model.

---

25   "Operation Inherent Resolve" Press Release (2017) "Coalition removes ISIS leaders from battlefield http://www.inherentresolve.mil/News/News-Releases/Article/1259778/coalition-removes-isis-leaders-from-battlefield/

26   This category includes research sites, jihadi monitoring sites, traditional media and individual CT researchers.

CONTAINING THE THREAT: GOVERNANCE CHALLENGES

THE POST 9/11 UK COUNTERTERRORISM STRATEGY

Jonathan Evans

Former Head of the British Security Service MI5. Currently, Director of HSBC Holdings, where he chairs the Group Committee on financial crime and cyber security, and member of the House of Lords.

Terrorism is a social and political phenomenon but it is also a practical public policy challenge. The UK, regrettably, has a long experience of terrorism, and its approach to terrorist threats in the last fifty years has been deeply influenced by its experience of, and response to, terrorism relating to the affairs of Northern Ireland. During the 'Troubles' in Northern Ireland from the early 1970s, the British state was faced at the same time with extensive sectarian and inter-communal violence in Northern Ireland, organised violent resistance to the state authorities in Northern Ireland, and an intermittent but persistent campaign of terrorist attacks in Britain, which over time included attacks on 'soft' civilian targets, attacks on public and military figures and attacks on the national and financial infrastructure of Britain.

The UK Counter Terrorist Strategy

The UK's response to the 9/11 attacks was therefore built on pre-existing policy assumptions, legal measures and institutional geography that had been developed over the preceding thirty years. The UK government's counterterrorist strategy, CONTEST, which was designed in the post-9/11 period under the leadership of Sir David Omand, then Security Co-ordinator in the Cabinet Office, who himself had worked on

Northern Ireland issues, is thus an evolutionary rather than a revolutionary document. It has also been remarkably resilient in policy terms – although there have been reiterations of the policy in the fifteen or so years since it was first agreed, its essence has remained unchanged and indeed the basic taxonomy that it applies in approaching terrorism has been recycled into the UK government's approach to other threats, notably serious and organised crime.

The CONTEST strategy consists of four strands, which are:

PURSUE – focussing on actions to identify, investigate, disrupt and where possible prosecute those who are engaged in terrorism or in the promotion of terrorism. This is work that falls principally but not entirely on the intelligence services, the police and the criminal justice system.

PROTECT – which aims to reduce the vulnerability of critical national infrastructure and other vulnerable sites to terrorist attack. PROTECT has had considerable success but as terrorist methodologies evolve PROTECT has also had to adapt. Protection of critical national infrastructure is a relatively defined problem but the vulnerability of public places to attack is more amorphous. The initial focus on reducing the vulnerability of the transport network and of major public events encouraged the terrorists to look elsewhere, in particular by mounting 'marauding' attacks such as those seen in Paris and more recently in the London Bridge area, or by using vehicles as a weapon as in Nice, Berlin and on the bridges of London. The PROTECT programme has therefore had to respond to these evolutions of the threat, and protective measures on bridges in London are now on the agenda. The problem for policy makers, however, is that the initiative for where to attack lies with the terrorists and the options available to them are more or less infinite. Therefore, vulnerabilities will always exist that terrorists will be able to exploit.

PREPARE – the level of damage that any particular terrorist attack can cause is related not only to the severity of the initial incident itself but also to the ability of society to respond to the attack and re-establish normal life afterwards. This is to say that the damage from terrorism can be reduced if we increase the resilience of our societies. In order to ensure that recovery from an attack is as rapid as possible, the government needs to be able to manage the initial crisis and to have available appropriate expert resources to manage the aftermath. The UK government has well-established crisis management arrangements headed by the COBR committee, which brings together relevant parts of government and the public sector to ensure that necessary steps are co-ordinated. Ensuring that the necessary resources are available to manage the aftermath is in itself a significant task: ensuring that the health services can respond adequately, that there are facilities to decontaminate after a radiological or chemical attack, that in the event of a large-scale loss of life it is possible to deal with the dead, and so on. This involves many parts of government that are less familiar with national security matters and these all need to be able to work together, sometimes with unfamiliar partners. Therefore, PREPARE involves a continuing and complex programme of work.

PREVENT – since terrorism is a complex social and political phenomenon, it is evident that a response to it which is solely based around traditional security techniques is unlikely to be wholly successful. While it is hard to imagine that the fissiparous, international and extreme groups that pose a terrorist threat today are ever likely to come together to negotiate a political solution to the grievances they believe they have, nevertheless it needs to be recognised that political, social and economic factors may have an influence on the extent to which terrorist groups are able to successfully promote their ideologies and to recruit new members both overseas and domestically. It

is therefore important to do all that can be done to push back against the extremist narrative and to bolster moderate voices within communities targeted by the extremists so that the terrorists' job of promoting extremism and recruiting new terrorists is made as difficult as possible. In many ways, this is the most difficult of the four strands of the CONTEST strategy since the levers available to government are limited, the outcomes slow to build, and most Western governments are ill-equipped to counter what are presented as religious arguments on the part of the extremists. As a result, the PREVENT programme is at the same time the most important, the most difficult and the most controversial of the CONTEST strands, and one where progress can be the most difficult to demonstrate.

From a personal perspective, I would add a fifth P to the CONTEST strategy, and that P stands for PERSEVERANCE. We have faced terrorism in Europe arising from Islamist extremism for over 15 years (and if you include the terrorist attacks in France in the 1990s arising from the Algerian crisis then for more than 20 years). Although the threat has increased and decreased periodically, and although the way in which the threat manifests itself has developed, as has its geographical footprint, overall there is no reason to think that the threat has been exhausted. This means that 'winning' against terrorism is unlikely, at least in the short or medium term. The threat is likely to persist. We need to develop policies that enable us to minimise and marginalise the harm that terrorists can do, and push back against their propaganda. However, this is a marathon not a sprint. At each step, we need to consider what the long-term effect of our own actions will be and refuse to take steps that will in the longer term play into the terrorist's hands. We should also continue to emphasise the resilience and stability of our societies, which in reality terrorists can do little to damage at the strategic level. While every attack is an outrage, and for victims

the impact can be horrific, we should not give terrorists the gratification of believing that their actions will ultimately destabilise or threaten our fundamental stability or our values. This means that we resolutely continue to take the necessary steps to counter terrorism but we also refuse to sensationalise or glamorise what terrorists are doing. Perhaps, surprisingly, President Trump has this right – the terrorists are 'losers'.

Themes from the development of Counterterrorism

The CONTEST strategy has set the framework for the UK's response to terrorism over the last 15 years, but I will highlight three themes that have also played out over the same period: resources, integration and technology.

RESOURCES. From a relatively low base at 9/11, the British government has spent billions of pounds on counterterrorism over a 15-year period. It spent around £800m on the security and intelligence agencies in 2000-2001. The equivalent figure in 2015-2016 was approaching £3bn. The budget is thus two and a half times larger allowing for inflation, and it continues to increase in real terms. Counterterrorist policing has also seen huge increases, and there have been increases in many other departmental programmes. Even discounting the costs of the military campaigns in Iraq and Afghanistan, counterterrorism does not come cheap.

INTEGRATION. The second theme of UK counter-terrorism over this period has been integration of effort. The three UK intelligence agencies have worked increasingly closely together as globalisation and the ubiquity of digital technology have challenged traditional institutional boundaries and made operational success dependent on close collaboration. The same drivers of change have brought integration between the intelligence community and law enforcement as both sides have recognised that their interests are aligned and that success follows

integration not separation. The same issues have driven closer international integration of law enforcement and security intelligence effort, both through bilateral exchanges and though more institutionalised structures. Again, there is no reason to think that this trend towards integration is likely to slow, as common threats require common responses. BREXIT is clearly a threat in this area but there is a strong interest on both sides to maintain links. This may be simpler for intelligence co-operation, where the arrangements are not within EU competence. Law enforcement co-operation through EUROPOL will require more formal renegotiation.

TECHNOLOGY. The third theme has been the increasing importance of technology in countering terrorism. This has gone hand in hand with developments in the digital sphere more widely across society, which have been exploited by terrorists, many of whom are now 'digital natives' and naturally turn to the internet to solve their problems and take forward their ambitions. While each step in technology can pose problems for the security and law enforcement authorities, each step also offers opportunities. The emergence of mobile telephony in the late 1990s was initially seen as problematic to the security authorities as it enabled terrorists and criminals to communicate easily from wherever they were in the world. It did not take long, of course, for the authorities to realise that it enabled them to track the location of suspects wherever they were in the world. Subsequently, communications data from mobile telephones have become a vital source of evidence in criminal prosecutions for all sorts of offences, as well as being a valuable intelligence resource. Of course, this has meant updating legislation so that the new opportunities open to the authorities are used on a legal, proportionate and accountable basis, but in the UK there has been a fairy broad political consensus that these powers are needed and should be available subject to the appropriate safeguards.

More complex has been the discussion over the use of bulk data as an intelligence resource. The reasons that this is controversial are obvious – that it involves the processing by the authorities of data relating to innocent citizens in order to identify the activities of terrorists and criminals. In practice, the actual level of intrusion involved can be limited through the anonymization of data in big data sets and the use that the techniques are put to can be subject to rigorous judicial scrutiny and accountability, but the issues arising are still complex. What is indisputable is that the mining of 'big data' provides a powerful way of understanding the world, including threatening activity within that world, which is why it is of such interest to commercial companies, whose 'big data' activities are much more extensive and less accountable than those of the security authorities.

Conclusion

For all the investment, technological innovation and legislative activity of the last 15 years, terrorism is still a real threat in Europe, both to the lives of our citizens and to the coherence of our communities. How much we allow it to be a genuinely destabilising force is to some extent in our own hands. Perseverance in our counterterrorist efforts will be vital but two things seem to me to be paramount. These two things are continuing to counter the grievance narrative of our enemies through words and deeds, and continuing to integrate our efforts. But integration and intelligence sharing are only as valuable as the insights that each partner can bring and there cannot be passengers. This means that all partners need to have the capabilities to investigate threats, deliver intelligence and take appropriate action.

TERRORISM AND THE NATO CONTRIBUTION

Jamie Shea[1]

Deputy Assistant Secretary General for Emerging Security Challenges at NATO

Terrorism may not be more dangerous but it is certainly becoming more complex and diverse. We are now confronting prepositioned ISIL cells and lone actors – some of whom are directed from Raqqa or Deir az Zour, while others are self-inspired. A few years ago, ISIL leader Abou Moussa al Suri predicted that terrorist attacks would come in the form of 1,000 small cuts, and this is what we are now seeing with a spate of small-scale attacks in London, Manchester, Stockholm, Paris, Brussels and Dortmund. Those likely to attack are vulnerable and frustrated, and some are mentally ill. Many attackers have a criminal past (812 confirmed hits out of the 5,000 foreign terrorist fighters who have travelled from Europe to Iraq and Syria). The role of the internet has increased in line with the 18-fold increase in internet traffic across borders between 2005 and 2012. The terrorists have used migration as a transit route and sought refugees as recruits. There are also more women (around 20% of the total) and converts involved in ISIL than ever before.

Our response has improved, but some 2,500 foreign terrorist fighters are still believed to remain in Iraq and Syria. Many have been or will be killed as the counter-ISIL coalition recaptures Mosul and Raqqa, but others will seek to return to Europe battle-hardened or relocate elsewhere and join other groups. Sinai and Libya are of

....

increasing concern and Sunni disillusionment with the way in which geopolitics seem to favour Shia or Kurdish interests against their community will facilitate the emergence of new Sunni jihadist groups, especially if the Iraqi government cannot achieve good governance, reconstruction and the return of displaced civilians to cities such as Mosul, Ramadi and Fallujah. Small groups may well fuse into a new Al Qaeda franchise and the recent focus on the elimination of ISIL's caliphate has meant that other well-armed and organized groups, such as Jabhat Fatah al-Sham, have been left largely unscathed. They have been developing advanced explosive devices, chemical weapons, drones with grenades, the miniaturization of components, dirty bombs and synthetic biotechnologies. The easy availability of online learning, through MOOC courses for instance, makes it easier for the jihadists to convert know-how into capability.

The continuing reality and ongoing metamorphosis of the terrorist threat are forcing the transatlantic partners to develop an ever-broadening spectrum of policy responses, reflecting the clear conclusion that military operations can never provide a long-term solution to terrorism. The EU, for instance, has pushed ahead with data collection and data transfer with the US (Privacy Shield), and also with the introduction of a passenger name recognition system for air travellers. It is striving to achieve a better balance between encryption and security and has engaged the major IT and internet companies in a voluntary arrangement to remove jihadist propaganda from the internet. In 2016, Google, Facebook, Twitter and Microsoft agreed to cooperate to develop a database where they will mark terrorist content with a specified identifier. Other companies can then see this tagged content and remove it from their own sites. In Britain, a specialist anti-terror police unit removed 121,000 pieces of terrorist content last year with the help of some 300 companies around the world. A similar referrals unit at Europol in The Hague has removed 30,000 pieces, with a 90% success rate vis-à-vis the

internet service providers. An Internet Forum is engaging the private sector in a discussion on how more and better counter-narrative material can be put on line as part of the EU's Prevent strategy. Some companies are experimenting with new tactics, such as Jigsaw, a sister company of Google, which has tested a 'redirect method' showing ads and videos to people looking for jihadist material on Google and YouTube. The Europol and Schengen databases are being better aligned and filled out with biometrics (with 8,000 names now on file). The EU is also working on digital proof and its exploitation through Europol and Eurojust. The gathering of forensic evidence from the battlefield is particularly crucial. This can help to prepare for future trials of ISIL and other jihadist leaders. In the meantime, Frontex and Europol are now working together to achieve better border controls and management.

On the external front, and in the wake of the Charlie Hebdo and Bataclan attacks in Paris, the EU member states have concentrated on their immediate neighbourhood, for instance Morocco, Tunisia and the western Balkans. The European External Action Service, the EU's Counter-Terrorism Coordinator and Europol's Counter-Terrorism Cell are setting up partnerships with most of the countries along the North African littoral, focusing on border management, aviation security, security sector reform, countering violent extremism and the rule of law. Under the Maltese EU Presidency, Ministers of Defence and of the Interior have met to better integrate the external military and internal police and intelligence services aspects of fighting terrorism.

This stepped-up level of EU activity, as well as the push from the Trump administration for NATO to have a more substantive and visible role in the fight against ISIL, has raised the question of the alliance's added value as an actor against terrorism. Consequently, in the run-up to the mini-summit that NATO's leaders held in Brussels last May, the 29 allies worked on an action plan to reflect

a higher level of ambition for an organization normally associated with classic conventional deterrence and defence against threats from nation states. What are its principal novelties?

In the first place, and following a long-standing US request, NATO agreed to join the Counter-ISIL Coalition. There had been some debate within the alliance about the added value of this step, as all the allies had previously been coalition members on an individual basis. Moreover, some allies worried that in joining the Coalition NATO might become involved in combat operations or even be called upon to replace the coalition in a big country like Iraq in the wake of the recapture of Mosul and the end of formal coalition air and ground operations. On the other hand, the prospect of a seat at the table together with 70 countries and other international organizations (including the EU and Interpol) at Coalition meetings, as well as the useful exchange of information and analyses on the evolving terrorist threat, finally sealed the consensus in favour of Coalition membership. NATO has offered to use its AWACS aircraft based at Konya in Turkey in a more forward-leaning role supporting not only air surveillance but also the coordination of air operations. At the time of writing, it is not clear what other tasks NATO might be asked to take on in the future. The Coalition's focus is overwhelmingly on the recapture of Raqqa and the final rolling up of the ISIL caliphate in other areas, such as in the Euphrates Valley, Deir az Zour and Al Tanf. There is as yet little indication as to which direction the Coalition will take post-Raqqa, other than a general acceptance that it will remain in existence. NATO is already in Iraq, with a modest training and advisory mission helping the Iraqi forces with counter-explosives expertise, military medicine and the repair of military vehicles and equipment. This activity could be ramped up but the Coalition is also carrying out a great deal of training of local forces with the participation of many non-NATO countries and may well decide not to disrupt

these ongoing activities. Moreover, as part of the US strategy review of Afghanistan and pressure from the ISAF Commander, General Nicolson, the Allies are being asked to find more troops for the Afghanistan Resolute Support Mission. An effective NATO training role in Iraq would require a military headquarters and operation with force generation along the lines of Afghanistan, (not to speak of the demands of NATO's Enhanced Forward Presence in Eastern Europe in terms of forward deployed troops headquarters and exercises and reinforcements). Consequently, these considerations might dampen NATO's enthusiasm for a greatly expanded commitment to Iraq.

Other items in the list of 38 activities in the action plan will be easier to implement. A new Joint Intelligence and Security Division within NATO has been established, which will not only bring more intelligence products into the headquarters but also combine better military and civilian intelligence flows. A cell dedicated to terrorism is now operating and NATO's battlefield intelligence distribution network (BICES) has been upgraded to handle biometrics and alpha-numeric information. A hub is also being established at the NATO Joint Forces Command Headquarters in Naples, which can combine intelligence fusion and assessment with the sending of mobile training teams to those partner countries in North Africa and the Middle East which participate in the Alliance's defence capacity-building and stability-projecting efforts. What part of the assessment should be carried out within NATO's military command structure in the southern region and what part at NATO in Brussels, close to the EU and the law enforcement authorities, is an issue still to be determined.

Where training and defence capacity-building do not require a military operation but only a lighter footprint, it will be easier for NATO to provide support to the countries of the Middle East and North Africa. Kuwait has offered the alliance a regional training centre, where it can organize courses. A regional crisis management centre has already been established in Mauritius and there are plans to create a similar centre in Iraq as a potential deliverable for the next NATO summit in 2018. A NATO presence can be financed through trust funds or can be handled by a lead nation willing to take on the overall responsibility, something which the UK has offered to do in Jordan. What the alliance now needs to do is to determine whether it wishes to have a training presence in a large number of countries or whether to conduct more in-depth training in a smaller number, such as Jordan or Tunisia, where NATO has already established close political relationships. For instance, in Tunisia NATO has been helping to develop Special Operation Forces and a reform of the intelligence services, and in Jordan it has been carrying out counter-explosives training and also helping Jordan develop its first national cyber defence organization.

NATO also needs to explore the relative benefits of different types of approach; for instance, to focus on mobile training teams or an in-country presence or out-of-country training and how these can be most effectively combined. Given the fact that a great deal of money has been wasted or misspent in recent years in places such as Iraq or Afghanistan trying to train and equip local forces which have then under-performed in conflict, not to speak of high levels of corruption in those armed forces, NATO will also need to conduct a serious lessons-learned exercise. It will be important to look at doctrine, concepts, resources and processes to better understand how investments can be made more productive and sustainable and where the balance lies between what NATO can realistically expect local forces to do by themselves and where the support of foreign armies remains critical. The lessons of the recapture of Kunduz in Afghanistan and Mosul in Iraq demonstrate that local forces work far more effectively when they are helped in the front line

by western special forces and are provided with air and artillery support, battlefield intelligence, drones and medical evacuation. This approach also favours NATO countries. Whereas the US has suffered nearly 3,000 military deaths since 2001 in Afghanistan, it has thus far lost only 11 soldiers in the recent operations against ISIL in Iraq and Syria. Given the prevalence of corruption in local forces, NATO's Building Integrity programme will need more funding and the alliance will need to direct its efforts precisely at those levels where it can be most influential. This would point to the development of leadership skills, doctrine and organization rather than the training and equipping of soldiers in the field, which arguably is done better by individual nations.

Finally, fighting terrorism will necessitate closer cooperation with the European Union. There are some things that NATO can do on its own without an EU contribution. Deterrence and defence in eastern Europe and nuclear burden-sharing are two examples; but counter-terrorism is definitely not one of them. Here NATO will be effective only in proportion to its ability to engage more closely with the European Union. This is obvious in the case of maritime missions to cope with migration, such as the operation in the Aegean that NATO is conducting together with EU Frontex and also its support to the EU Sofia mission in the central Mediterranean, where both organizations are coordinating patrolling, logistics support and intelligence-sharing. If NATO begins a new mission in Libya in the near future (and the Libyan government has requested NATO support), this only makes sense in cooperation with the European Union, which will need to take responsibility for border management and the setting up of a new police service and judiciary. Libya is too big and too complicated for NATO to handle by itself and the resources of the EU for development aid and institution-building far outstrip what NATO has in its commonly funded budgets. On the other hand, NATO could also help

the EU. The collection of battlefield intelligence would help the EU to track returning foreign fighters, and the experience of fighting piracy in the Gulf of Aden has shown how NATO assets, such as observation drones, biometrics collection and weapons intelligence can be useful to EU law enforcement, particularly Europol. Last year, at its summit in Warsaw, NATO agreed a joint declaration with the EU to enhance interaction in 42 specific areas. These provide for more cooperation on capability development, hybrid warfare and cyber security, but the declaration is relatively thin on counter-terrorism cooperation. This is an area that could be further developed as another deliverable for NATO's summit next year. Apart from Libya and maritime operations, NATO and the EU could consult more closely on capacity-building, particularly in North Africa. Could NATO support the new G5 regional group that France has helped establish in the Sahel? What about more joint analysis and information-sharing? Or closer cooperation with Europol (which incidentally would be useful in the area of cyber crime, as well as counterterrorism)?

In conclusion, NATO's future role in counterterrorism will depend on two factors. The first is its ability to develop a coherent and long-term strategic vision for the south and the programmes and resources for effective capacity-building in a large enough number of countries to achieve a lasting strategic impact. The second is a closer working relationship with the EU, which could not only extend to North Africa but which could usefully cover parts of the western Balkans, such as Bosnia or Kosovo, from which many foreign fighters have left to join ISIL. The political pressure for the alliance to raise its game is definitely there and as NATO's recent mini-summit showed, it comes not just from President Trump but from many European allies, who notwithstanding Russia's incursions into Ukraine and Crimea continue to see terrorism as the number one threat. NATO's action plan is a good

start, but as one NATO leader said at the recent Brussels meeting, "we need to put the action into the plan." To this, I would add "and look at further steps in the near future."

NATO BROODS ON COUNTER TERRORISM

Juliette Bird[1]

Head of NATO's Counter Terrorism section

The European Union's mandate enables it to cover almost as many counter terrorism (CT) related issues as its component nations; by contrast, NATO's range is more modest and is firmly located at the military end of the CT spectrum. But both organisations have unique strengths and a duty to contribute as effectively as possible to the international effort against terrorism. In May 2017, the leaders of all the NATO nations endorsed a report on NATO's CT role to date and a challenging new Action Plan of measures designed to enhance NATO's overall contribution. Despite the profound resolve of NATO nations in the field of CT, external commentators continue to see the Action Plan as a response to pressure from Donald Trump conveyed in a series of tweets in 2016 and 2017.[2] In this context, this short piece by Juliette Bird adopts an avian theme as it sets out where NATO has got to and where it is headed as it plays its part in the international fight against terrorism.

First flight

In 2001, NATO lurched into the void like a fledgling, taking its first and most dramatic action against terrorism in response to the 9/11 attacks on the United States. This external attack on an ally prompted NATO's first, and to date only, use of the collective defence mechanism provided for in Article 5 of its founding treaty. The attack and the need for a response came as a shock to the NATO system; terrorism had not previously been viewed as a major threat and no policy, doctrine or staff structures were in place, and neither had NATO's intelligence structures been consistently focused on the issue. A hastily constructed Military Concept for Defence against Terrorism provided a basis for NATO deployment in response to terrorism and two so-called 'Article 5' operations were launched, backfilling US AWACS[3] capacity and patrolling the Mediterranean to limit terrorist access to non-conventional weapons.[4]

In only a slightly longer time, NATO then reviewed and re-evaluated what it did, or could do, of relevance to countering terrorism. Its focus was initially on ensuring a rapid military response (through the NATO Response Force), improved intelligence sharing and measures against non-conventional (CBRN) and explosives attacks, but it also reached out to partners, seeking a fuller picture of the terrorist threat and others' experience of counter-measures. Subsequently, NATO invested in Consequence Management, Civil Emergency Planning, Critical Infrastructure Protection and the development/deployment of new technologies against asymmetric attacks.

Thereafter, NATO perched, surrounded by familiar issues, many of them previously mainstream activities but now labelled 'CT,' in a more-or-less settled fashion for ten years, still without a CT policy or a dedicated staff structure. This may seem extraordinary in retrospect, given the current context, but NATO, like all international organisations, only mobilises on a specific topic when there is a groundswell of high-level political attention, and there were seemingly more pressing issues at the time (e.g. in Afghanistan and the Balkans).

---

1   This paper was first delivered to the Conference on Terrorism and European Security Governance of the European University Institute in June 2017 as the author's own views. It is not an official NATO position.

2   In March 2016, then presidential candidate Donald Trump tweeted "NATO is obsolete and must be changed to additionally focus on terrorism…."

3   Airborne Warning and Control System

4   Operations Eagle Assist and Active Endeavour

Nest building

Even the best perch can only ever be temporary and for NATO to have a stable long-term approach to CT a stronger base better adapted to its surroundings was needed. The CT environment had indeed changed in those 10 years: United Nations (UN) Security Council resolutions, especially 1263 , had pushed nations to create and begin to implement their own CT strategies; the EU put one in place in 2005; and in 2006 the UN reached agreement on a Global CT Strategy. So, it was rather late in the day, in 2010, that NATO assigned staff to a CT section and undertook a full review of the relevant terrorist threats and of its own strengths together with a gap analysis, looking for NATO-shaped holes amongst the roles of other international organisations. The findings were then structured and put forward for allied approval.

The outcome was NATO's CT Policy Guidelines,[5] endorsed by Heads of State and Government at the Chicago Summit of 2012. NATO was tasked to address three pillars: Awareness of the threat (through intelligence exchange, consultations etc.), Capabilities (to ensure NATO action remained possible despite the terrorist threat) and Engagement with partner nations and other international organisations (to ensure a cohesive international approach). Everything NATO was directed to do was to be in support of its allies but still many found aspects of a NATO CT role uncomfortable, particularly those who viewed CT as a strictly domestic challenge. There was little desire for a public profile for NATO on CT and no dedicated strategic communication approach was to be attempted. Likewise, there was no appetite to point to any CT value arising from NATO's missions (e.g. Afghanistan, the Balkans and later Libya and the Horn of Africa) except (as in the case of Active Endeavour in the Mediterranean) if the mandate was specifically CT-related.

5   NATO CT Policy Guidelines http://www.nato.int/cps/en/natohq/official_texts_87905.htm

Faced with these caveats and very varied levels of national interest, annual progress reports put to the allies together with proposals to increase NATO's level of CT ambition achieved only modest increments of progress – until the tweeting started and the prime tweeter became a President.

Twittering and crowing

The basic Trump criticism of NATO on CT was largely unwarranted. NATO has clear value to add to the efforts of nations and other international organisations and was already working within the CT field with a large community (some 70 nations) of both partners and allies. As the Wales[6] and Warsaw[7] summit declarations make plain, CT had been recognised as an aspect of the broader NATO flagships of Deterrence and Defence and Projecting Stability. Nevertheless, the need for an international response to the threat from ISIS/Daʾesh, concerns about radicalisation, home-grown terrorism, foreign terrorist fighter flows, the deterioration of the situation in Iraq etc. prompted NATO, and many others, to launch a review of what more could be done.

Egg laying

In spring 2017, allied discussions started in earnest and, almost 30 committee meetings and formal or informal meetings of the North Atlantic Council later, a report of NATO's strong points and achievements to date accompanied by a 38-point action plan was agreed and presented to Heads of State and Government in May for endorsement. The clutch of 38 actions are grouped under seven pillars: awareness and analysis, preparedness and responsiveness, capabilities, capacity building and partnerships, operations, governance and strategic communications. Many of the tasks are

6   Wales Summit Declaration http://www.nato.int/cps/fr/natohq/official_texts_112964.htm?selectedLocale=en

7   Warsaw Summit Declaration http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

predominantly for internal action but, especially for an external audience, the following five areas have particular importance and are worth highlighting.

1. Recognition of the CT-impact of NATO missions and operations whether or not the mandate includes a mention of terrorism. Contributing to stability, capabilities and capacity-building of states (e.g. through the Resolute Support Mission in Afghanistan, Sea Guardian, assistance to Iraq and support for the Global Coalition to defeat ISIS) is now appreciated for its CT-relevance. NB NATO was welcomed as a full member of the Global Coalition immediately after the May 2017 meeting.

2. Appreciation of the CT-relevance of adaptation already underway at NATO as part of the effort to be better aware of developments to NATO's south and better positioned and prepared to be able to engage e.g. on Libya. The Hub for the South based in Naples reached initial capability in September 2017 and will contribute to enabling CT-relevant support to be provided to partners in the region.

3. Commitment to a more systematic approach to training, advising and assisting partners on CT. This is part of a wider NATO approach across a variety of topics under the Projecting Stability banner, using all relevant assets where appropriate e.g. Special Forces, Centres of Excellence etc.

4. A focus on intelligence that does not just belabour the 'share more' point but has practical deliverables. This includes the creation of a Terrorism Intelligence Cell, the making available of information from operational theatres to allies domestically and the use of Joint Intelligence, Surveillance and Reconnaissance assets where they can be helpful against terrorist activity.

5. A firm resolve to be more joined up with the overall international effort. A strong focus on the EU, but also more widely to ensure more engagement with the Organisation for Security and Cooperation in Europe (OSCE), the Global CT Forum (GCTF) and INTERPOL, and to initiate CT relationships with regional organisations such as the African Union, Gulf Cooperation Council, G5 Sahel and ECOWAS.

These are combined with a (perhaps overdue) realisation that better public awareness of NATO's role could be helpful, as not only the US but other allies too are asking for NATO to have a more visible role. A communications framework is now under development.

Any chicks likely?

The level of ambition captured in the Action Plan was not arrived at without a struggle and is as challenging as consensus decision-making allows. This means that it is daunting to some allies and disappoints others. There are still those who would rather not use NATO for CT except *in extremis*, preferring to act alone, in ad hoc coalitions or through the EU. Some allies are averse to non-permissive environments, most are economically constrained and everyone jostles to see their favourite partner nation or organisation benefit from new initiatives, so the implementation process is bound to be interesting.

Will NATO be able to take this set of intentions through to fully fledged activities? One thing is sure: it will not be for want of trying at the institutional level. As an indication of high-level resolve, the Secretary General has already appointed his Deputy, Ambassador Rose Gottemoeller, as coordinator to drive the effort

forward. But only allies are able to ensure that the environment will indeed be conducive to effective egg-hatching. Will the resource situation be comfortable enough? Will the engagement be consistent enough? Will the political attention span be long enough? Or will bird brain responses complicate matters?

Counting chickens

NATO's review cycles for CT are becoming shorter: the first took a decade to come round, the second only half that, and the next is likely to follow in two to three years' time. What there will be to commend next time round will, as has been said, depend on national engagement, resourcing and persistence. Whilst the future can never be certain, NATO should at least be recognised in 2017 for an effective overhaul and relaunch of its CT effort that is coherent with the overall international approach. It has not succumbed to the temptation to divert its efforts into areas better addressed by others. Counter- and de- radicalisation are not NATO's strengths and the financing of terrorism, social media counter-messaging and improved law enforcement are definitely best left to others. But what NATO has in the way of unique assets, at the military end of the spectrum, it has committed to use wisely and as part of the greater whole. Against terrorism, as with many security challenges, the universal aspiration should be to ensure that national, international, internal, external, civilian and military aspects of prevention and response are seamlessly joined – a far from trivial task but one in which NATO, the EU and others can have an important influence.

THE RECENT DEVELOPMENT OF EUROPOL: AN ALTERNATIVE TO A EUROPEAN FBI?

Wil van Gemert

Deputy Executive Director of Europol and responsible for the Operations Department.

Introduction

At the age of 18 it is generally assumed one reaches the status of adulthood. It is often the case that one's physical appearance and self-consciousness change significantly in the years prior to this. Whether this also applies to organizations is probably questionable. However, the fact is that Europol just recently turned 18 years old and during the last three years a big change in positioning and role for the organization has taken place. This article covers developments as they unfolded in the area of European law enforcement and the way in which they have impacted the role and positioning of Europol and instigated change.

Europol as an organization: the crown jewels

Europol, or more specifically the European Police Office, as the organization has formally been called since 1 May 2017, is the agency of the EU which aims to improve and support police cooperation in Europe, thereby increasing the safety of its citizens. The agency is housed in a modern and state of the art building in The Hague, where, currently, already more than 1000 people work. Europol focusses mainly on cross-border organized crime, terrorism and cybercrime. At

the time of the creation of the European Union and the opening of borders, it was a logical consequence to simultaneously strengthen police cooperation through better data exchange. The Schengen Information System (SIS) can be seen as another tool to support this cooperation. Both are responses to reduced border controls and responsibilities of the individual countries.

In order to perform this task properly, Europol has a number of resources. The most important ones, and those which could be considered her current crown jewels, will be briefly outlined below.

The largest liaison community in one building in the world: One of the most important principles at Europol's creation was that in addition to creating an agency there would also be representation of the Member States on site. This principle of 'desks' to represent the Member States has grown into a community of more than 200 liaison officers from 43 countries. These include not only the 28 Member States but also other important partners with which Europol has predominantly operational cooperation agreements. These are countries like the US, Canada, Australia and Columbia, and also Norway, Iceland, Switzerland, Serbia, Albania, etc. These liaison officers are formally not part of Europol but are employed by their own governments and supported and housed within the Europol building. This is a unique facility which, for example, allows police officers confronted with unknown factors in an international case to ask questions in their own language and have the questions communicated in English to the dedicated representative of the other country. With the knowledge of the national organisations in the countries at hand, there is assurance that the questions will subsequently be addressed to the right person. The potential of this instrument is huge, not only when it comes to individual questions but also for the exchange of information in the case of an emergency or when a large-scale incident or attack occurs. Representatives of all the countries can be brought

together in an operations room within 15 minutes. As an illustration of the recognition of the value of this 'place to be,' the US is now represented at Europol by 11 agencies and 18 permanent and 7 temporary liaison officers.

Its databases: Since its inception, Europol has been exchanging and storing information about suspects and crimes. Member States and operational partners can 'subscribe' to the various analytical projects and in doing so commit themselves to recording data on the projects. These databases currently include almost 30 different crime areas, ranging from all forms of drug crime, firearms, trafficking in human beings, terrorism and extremism, and the various forms of cybercrime, including fraud and sports corruption. Very soon an analytical project in the field of war crimes will be launched. The information is stored under a strict data protection regime, is regularly evaluated, and has since expanded to more than 28 million items. This is an important source allowing Europol to make connections between ongoing investigations. Approximately 5,000 analytical reports are produced annually, in either extensive or limited format, and they are sent to the stakeholders by Europol.

The secure connection system – SIENA: Currently with more than 7000 users and 700 connected national units, competent authorities and organizations, a system is needed to allow the secure exchange and communication of information. The Secure Information Exchange Network Application (SIENA) is a secure and efficient connecting system through which approximately 20,000 messages are exchanged on a weekly basis. This may be bilateral data exchange but it may also entail informing all Member States about concrete cases, changes in *modus operandi*, or important information about incidents. Europol receives approximately 2,000 weekly messages, which, after verifying that the information falls within the mandate, are accepted and processed.

The expertise role: Focussing on nearly 30 different organized crime areas and having the ability to recruit operational staff from 28 Member States, Europol must be in a position to be able to acquire the latest expertise and knowledge in these fields. The majority of the staff in the Operations Directorate are either specialists or analysts. More than 120 analysts are involved in analysing the information in the various analytical projects. The specialists are expected to have background knowledge in the different task areas and to be able to produce 'early warning' reports on changing *modus operandi*. The latest expertise is also available in areas of forensic engineering, social media and strategic analysis.

The Coordination Task: With an overview of more than 1,000 'high profile' investigations and assisted by the aforementioned means, there is the possibility of coordinating and de-conflicting between the various investigations. Also in the field of EMPACT (European multidisciplinary platform against criminal threats) priorities, the primary criminal areas chosen by the European Union, Europol plays a role by coordinating investigations and the activities to be launched. For this purpose, it is possible to create an operational coordination centre within a few hours or to use, for example, the three equipped operations rooms. Actions like Archimedes and Ciconia Alba are some good examples. The recent takedown of the two biggest dark markets, Alpha Bay and Hansa, are examples of better results being achieved through international coordination.

The development of these 'crown jewels' and, at the same time, the situation in Europe since 2015 in which migration and terrorism have increasingly determined the agenda have led to Europol developing a different position and role in the field of investigation. One of the most important 'game changers' is the rise of cybercrime. This is an area where international cooperation is always necessary but at the same time where Member States do not always have the necessary knowledge.

EC3, the Cyber Centre established 5 years ago, can be seen as a forerunner in this area and it steered Europol onto a new course. Currently, many new developments and initiatives are rooted in the cyber environment and are then applied in other areas.

Europol's changing roles

With regard to Europol's new positioning, in my view three important roles can be distinguished:

1. Europol from information warehouse to supporter in the complete investigation cycle

Whereas in the first instance Europol's task was primarily seen as providing for information exchange and the setup of relevant databases, this role has changed over the last few years. Partly due to the possibility of having operational meetings financed, Europol is now also involved at the start of investigations, during progress discussions and in the operational end-phase. Europol remains involved even after an investigation has been completed. This support includes not only being on the spot with a mobile office to directly check information but also supporting data retrieval, giving forensic support and providing expertise in, e.g., drugs lab dismantling, analysing confiscated data and making reports, which can also be used immediately in court. Another important application is the handling of seized material in an internationally coordinated action. The best example of this is probably the Victim Identification Task Force. This is an annual action where in one joint effort and over a period of 14 days information that is not linked to national targets related to child pornography networks is analysed. More than 20 countries were involved in the last action in 2017. In the space of two weeks, 40 detectives analysed the information they had brought with them using the Europol forensic network. These actions have already led

to the identification of more than 40 children who, without any doubt, would otherwise not have been identified and taken away from the situation of abuse. In addition, after the attacks in Paris and Brussels, the way in which a Europol task force called Fraternite delivered direct operational support for 1.5 years and was part of the Joint Investigation Team (JIT) illustrates a role newly required of Europol, one which Europol offered.

2. Europol as an alternative to an EU investigative body, or the need for European policing;

In recent years, the call for a European style FBI has been heard several times. This has mainly had to do with the need of, e.g., the European Parliament or other authorities to have priorities better defined as an answer to, in their view, failing investigations. As a professional, I do not think this is the solution. However, there is a need to do things in a uniform European way or to gain insights at the European level. This became most clear to Europol when in 2015/2016 the asylum flow within Europe manifested itself. Frontex had a clear view of the number of incoming migrants at the borders, but not within the EU. As a consequence, at the request of the Member States, Europol drafted a daily monitoring report to reflect developments within the EU and thereby support police activity. The same need exists with respect to, e.g., standards in the field of e-evidence and the analysis techniques used. Future initiatives such as ETIAS and PNR also highlight the need for a European centre in which tools such as a watch list are set up. A centre for enhanced cooperation and standardization together with a 'one-way stop' for private partners or other institutions where EU-wide interests in the area of law enforcement are concerned is required. In my view, Europol can and should fulfil this role.

3. From collecting towards more connecting

As a data processing agency, Europol is very active in the business of 'collecting' information. In recent years, we have seen a huge increase in this area. For example, the amount of information shared by Member States and third states on foreign fighters has grown tenfold in the last 2 years. In other areas too, we see an increase in the quantity of information received with quarterly growth between 20% and 25%. This trend has certainly been continuing for the last 2.5 years. In addition, the number of messages sent via SIENA will be over 1 million this year. In 2014, it was only 605,245. A similar increase can be seen in consultations of EIS, the Europol Information System. Although this development is very encouraging, it appears that, in addition to gathering information, connecting the various databases available is becoming more and more important. It is not surprising that a High Level Interoperability Working Group was set up at the European level last year. The aim of this group is to explore how existing systems such as SIS II, VIS and PRUM can be better aligned and used. Furthermore, the amount of data available has increased exponentially. It is therefore a question of better use of data already available in other systems, like, for example, at the FIUs. It is an illusion to think that all this data should still be stored in one big central data system. We also notice a similar trend in mainstream industry to focus more on connecting, real-time access and cloud applications. This means that Europol is increasingly profiling as a connector and supporter of information. A good example is its acquisition of the FIU support unit and its maintenance of the FIU network. Recent attacks have shown that the main problem is a fragmentation of information rather than a lack of availability of information on criminal suspects.

In my view, these three developments characterise the changing position of Europol. I am convinced that developments will continue, partly through new initiatives that are being undertaken and partly owing to changes in society and their impact on the fight against organized crime.

Other cooperation in the area of terrorism

The developments outlined were intensified by the attacks in 2015. On the evening of 13 November 2015, directly following the attack, an Incident Response Team was set up at Europol and in the following weeks its staff grew to 60 members. At the request of France, operational on-the-spot support was immediately provided, together with analysis of the information available. In the course of the following months, more than 19 terabytes of information from France and Belgium was submitted to Europol. The focus was put on identification of the support network, travel movements and the international dimension. Simply stated, whilst the national research teams focussed more on who did what and where, Europol concentrated more on why, how and what will follow. Europol is still working on these cases and already more than 120 analysis reports have been drafted.

The same approach and support was repeated in subsequent investigations, amongst others in Brussels, Copenhagen and Berlin, thereby creating a support platform for the establishment of the European Counter Terrorism Centre (ECTC). By, amongst other things, applying methods that have already proven to be successful in tackling cybercrime, such as joint liaison teams of operational staff, the collating of operational information, the extension of several databases and a strong focus on social media and financial information, ECTC has in a short period of time established itself as an important support and facilitation centre. The databases that have now been created are an important source for all current and future investigations into terrorism. Furthermore, by collaborating with partners such as Interpol and non-EU countries, the

amount of information has grown exponentially. As such, ECTC provides an important base for strengthening future operational cooperation in Europe in the area of combatting terrorism.

The Future

I would like to conclude by providing some examples of similar developments. The need to face European threats at the European level requires enhanced cooperation and the prevention of duplication. Existing partnerships such as ATLAS (the agency in which the SWAT teams work together in Europe) are looking for a partner to join so they can use its infrastructure and support possibilities while keeping their own identity. Greater cooperation between European intelligence services, in a premature form of a fusion cell, will also lead to some type of cooperation with their counterpart in the area of investigation, i.e. Europol.

The development of society to one in which citizens are becoming more and more global means that for the management of contacts, connections, overstays and financial flows they make use of infrastructure which is no longer owned or accessed by national authorities. Where in the past the national telecom company or hotel reservations could be accessed through national systems and national legal orders, Google, Bitcoins, Facebook, Whatsapp and Air BNB now represent substantial problems for investigative authorities. How to retrieve information from these companies is relatively unknown and complicated. Conversely, these companies need a supra-national approach instead of making arrangements with each and every single government. Here too there will be an increasing need to act more through an organization such as Europol. A first experience of this already exists at the level of the Internet Referral Unit, which is part of Europol, and partly plays an overarching role in this area. New initiatives are also being born, like the development of Sirius, a tool that should provide a solution exactly in this area.

In short, Europol acts in a very dynamic environment. Whether it should exist is no longer in question. It is now all about defining the boundaries and the right demarcation. This makes the role and developments of Europol only more interesting.

Publications Office