Shadow orders: clandestine non-state power in the international system

Bastrup-Birk, J.T.N.

CHAPTER 5 – Levers of power

This third framework chapter focuses on the various instruments of power that allow clandestine non-state actors to translate and convert policy objectives (Chapter 3), via operational structures (Chapter 4) into real-world activities and effects. In doing so, it provides a basis for investigating the thesis' third hypothesis, namely that these actors consistently apply a variation on the types of levers available to states, albeit typically at a smaller scale, including with respect to the conduct of warfare, the pursuit of economic and financial interests, and strategic communications. Building on this analysis, the chapter argues that in today's highly connected world, even smaller groups can increasingly operate on a wider scale by both harnessing readily available, 'off the shelf' capabilities and expertise and by leveraging the services of a global network of logisticians, professional service providers and field operatives. In doing so, these actors are arguably able to deploy means that were previously available only to state actors, somewhat levelling the playing field between the state and sub-state levels. In reality, such capabilities are often applied in concert as part of sequenced campaigns of influence. Clearly, clandestine organisations may not *necessarily* use all of the levers and instruments outlined below but may instead draw on these selectively or partially in pursuit of their respective objectives.

5.1 Violence and the use of force

The use of violence is often cited as one of the defining characteristics of clandestine non-state actors, distinguishing them from other types of non-state organisations. For example, the likes of Igor Primoratz argue that the use of violence (or the threat thereof) effectively constitutes the defining feature of terrorism.[379] Insurgency scholars similarly highlight the extent to which conceptual understandings of the phenomenon are rooted in such actors' propensity to engage in armed and violent activity.[380] Criminologists have also at times been quick to highlight the extent to which violence formed an integral part of criminal strategies. Thus, Gilbert Geis notes that "violence in the world of organised crime has been more common than in other segments of the social structure."[381] Despite these common perceptions, and as we have already seen, clandestine non-state actors are not automatically pre-disposed towards violence, which is instead guided more often than not by deliberate policy choices as well as rational assessments relating to the ways of achieving their objectives. In this respect, Phil Williams' claim that violence, whilst "latent and often manifest, […] is not integral to the criminal activity," could therefore be applied to the wider cast list of clandestine actors.[382] Moreover, Alex de Waal's concept of 'political marketplaces', within which violence constitutes only one function (or, indeed, transactional currency) at the disposal of so-called 'political entrepreneurs', also injects helpful nuance into the debate.[383] All the same, it remains true that clandestine non-state actors regularly opt to employ violence for reasons and in ways that merit closer examination.

---

[379] I. Primoratz*, What is Terrorism*?, Journal of Applied Philosophy, Vol. 7, No. 2, 1990, pp.129-138.
[380] See for example R. M. Wood, *Rebel capability and strategic violence against civilians*, Journal of Peace Research, Vol. 47, No. 5, September 2010, pp. 601-614; and F. Trebbi and E. Weese, *Insurgency and Small Wars: Estimation of Unobserved Coalition Structures*, Econometrica, Vol. 87, No. 2, March 2019, pp. 463-496.
[381] G. Geis, *Violence and Organized Crime*, The Annals of the American Academy of Political and Social Sciences, Vol. 364, March 1966, pp. 86-95. For more contemporary accounts see for example: M. Caparini, *Conflict, Governance and Organized Crime: Complex Challenges for UN Stabilization Operations*, Stockholm International Peace Research Institute (SIPRI), December 2022, p. 8.
[382] P. Williams, *Illicit markets, weak states and violence: Iraq and Mexico*, *Crime, Law & Social Change*, Vol. *52*, Issue 3, September 2009, pp. 323–36.
[383] A. de Waal, *Introduction to the political marketplace for policymakers*, Justice and Security Research Programme (JSRP) Policy Brief, London School of Economics and Political Science, March 2016, p. 3.

On the whole, analysis of the application of violence by different types of organisations points to broad coercive logic aimed at catalysing behavioural, attitudinal or systemic change amongst targeted parties.[384] In the case of terrorist, insurgent, guerrilla and rebel groups this is often – but by no means uniquely – directed at state actors such as governments and their security forces, thus demonstrating to their support bases that they can challenge the authority of these same protagonists. Criminal violence, meanwhile, may well be aimed at these same targets, such as in the case of pre-electoral violence aimed at influencing electoral outcomes or the behaviour of politicians (the Sicilian Mafia being a case in point).[385] However, it also constitutes a means of securing one's position within illicit markets and fending off competition, as witnessed in the case of the US Prohibition, Mexico's cartel wars or, famously, Pablo Escobar's campaigns of intimidation using legions of hired guns, so-called *Sicarios*.[386] Moreover, both categories of actors also use violence and acquire offensive capabilities for the purposes of deterrence and protection, with the aim of dissuading challengers (state and non-state) from potential aggression. Nevertheless, the acquisition of such capabilities for deterrence purposes arguably runs a risk of catalysing smaller scale manifestations of International Relations theory's 'security dilemma', where the defensive actions of one actor are interpreted as offensive or aggressive by another, potentially resulting in spiralling escalation.[387]

Clandestine non-state actors in the modern world are able to draw on a range of offensive capabilities, tools and weapons systems when seeking to engage in armed activity and acts of violence. From a purely tactical perspective, few capabilities have been as instrumental to clandestine organisations as the Kalashnikov AK-47 (and variants) automatic assault rifle.[388] The weapon, which was mass-produced by the Soviet military as a low cost, easy to use and reliable weapon system, became an icon for liberation movements in the wake of the Vietnam War. It has also been the weapon of choice for international terrorist groups dating at least to the 1972 Munich massacre, in which members of the Black September Palestinian group took eleven members of the Israeli Olympic team as hostages.[389] Current worldwide estimates place the current number of AK-47s at up to 200 million and, by the time of the Paris attacks in 2015, most terrorist and insurgent attacks worldwide were conducted using the weapon. As a result of its large numbers, the rifle is relatively easily easy to acquire: 750,000 disappeared from Albania alone following unrest in 1997.[390] Moreover, the traditional symbolism attributed to the AK-47 has become a regular feature of modern terrorist propaganda material, often propped up against the wall in the background of videos whilst leaders deliver *Fatwas* or rally followers to their cause.[391]

Demand for the AK-47 and other firearms has, in turn, opened niche business opportunities for those able and willing to source, smuggle and sell such weapons to buyers around the world. The black market for these weapons links 'supply' countries such as Albania, Libya and (perhaps ironically) the United States to both violent non-state actors and criminal

[384] See for example J. Waldron, *Terrorism and the Uses of Terror*, The Journal of Ethics, Vol. 8, No. 1, 2004, pp.5-35; and G. Duncan, *Drug trafficking and political power – oligopolies of coercion in Colombia and Mexico*, *Latin American Perspectives*, Vol. *41, Issue* 2, March 2014, pp. 18–42; and
[385] A. Alesina, S. Salvatore and P. Pinotti, *Organized Crime, Violence and Politics*, The Review of Economic Studies, Vol. 86, Issue 2, March 2018, pp. 457-499.
[386] J. Mollison, *Rise and Fall of the Cocaine King*, The Guardian, September 2007.[387] C. L. Glaser, Charles, *The Security Dilemma Revisited*, World Politics, Vol. 50, No. 1, October 1997, pp. 171–201.
[387] C. L. Glaser, Charles, *The Security Dilemma Revisited*, World Politics, Vol. 50, No. 1, October 1997, pp. 171–201.
[388] The Mumbai attackers carried AK-56 Chinese versions of the AK-47.
[389] M. Hodges, *AK47: The Story of a Gun*, San Francisco: MacAdam/Cage Publishing, 2007, p. 82.
[390] S. Laville and J. Burke, *Why has the AK-47 become the jihadi terrorist weapon of choice?,* The Guardian, December 2015.
[391] The weapon was used in this way by Boko Haram, al Qaeda and ISIS.

organisations in a global trade that could be worth as much as USD3 billion per annum.[392] Interestingly – albeit perhaps unsurprisingly – almost all of the weapons available on the black market were either manufactured under government control, originated from military stockpiles or purchased by licensed gun dealers.[393] The weapons smuggling market includes brokers with international reach and connections, as well as geographic logistical centres benefitting from transport links or from permissive legislative frameworks. For example, relatively soft penalties for converting deactivated firearms in the Czech Republic and Slovakia has turned the countries into an important production and distribution centre for guns subsequently smuggled to organised crime and terrorist groups in Western Europe.[394]

As we have seen, in the 21st Century, even organisations with a narrower geographic focus have the advantage of being able to combine traditional, tried-and-tested principles of asymmetry and guerrilla tactics with new technologies and tactics drawn from across the world. An example of this trend is the growing use of Improvised Explosive Devices (IEDs) globally. Such devices have both literally and figuratively exploded across various theatres of operation as part of both insurgent operations in conflict zones and terrorist attacks against civilian populations. Drawing on readily available bomb-making manuals and guidance, the devices can be manufactured from basic ingredients and components such as homemade explosives, fertiliser or artillery shells. These can also be configured to be employed by individual suicide bombers, deployed as car bombs, laid out on routes employed by military or government personnel, and/or detonated remotely using a variety of methods ranging from mobile phones and command wires to pressure plates.[395] Additionally, IED-manufacturing has broadly matched the development of countermeasures, as seen in the case of the Explosively Formed Projectiles (EFP) – copper slugs travelling at high velocity and designed to pierce through heavy armour – that were used against American troops in Iraq (the technology was allegedly introduced to the Iraqi insurgency by the Iranian Quds Force).[396]

Building on de Waal's concept of 'marketplaces', the provision of violence and protection may either be developed in house or outsourced to specialist providers (in a similar way to, say, states' use of private security companies and militias). Illustratively, the likes of Wolfram Lacher[397] and Matt Herbert[398] describe how, in contexts such as Mali, Libya and Tunisia, criminal and smuggling organisations have turned to armed militias and terrorist elements for protection. Clearly, this dynamic also introduces a potential area of overlap and intersection between state and non-state actors to the extent that both players may theoretically acquire the services of the same specialist (non-state) protection providers when pursuing their respective interests. For example, Lynette Ong points to the ways in which criminal elements are regularly deployed as third-party instruments of repression by local governments in China

[392] Based on estimates outlined in N. Marsh, *Two Sides of the Same Coin? The Legal and Illegal Trade in Small Arms*, The Brown Journal of World Affairs, Vol.9, No.1, Spring 2002, pp. 217-228.
[393] *Ibid*, p. 223.
[394] This was the case weapons used in the Paris attacks. See also M. Townsend, *From a Czech warehouse to a street near you: the journey of a gun*, The Guardian, 18 November 2018.
[395] An additional tactic favoured by insurgents is the so-called 'daisy chaining' of explosive devices connected to one another so that the detonation of one device along the chain would trigger that of others, potentially inflicting damage on a number of different targets such as armed vehicles in a road convoy or infantry soldiers on foot patrol. A. S. Hashim, *Chapter Four: Organisation, Targeting, Operational Art and Tactics*, The Adelphi Papers, Vol. 48, Issue 402, 2008, p. 48.
[396] P. McLeary, *Get the Facts Straight on Iran and EFPs*, Columbia Journalism Review, April 2007, available online at: https://archives.cjr.org/behind_the_news/get_the_facts_straight_on_iran.php.
[397] W. Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*, Carnegie Papers, Carnegie Endowment for International Peace, September 2012, p.8
[398] M. Herbert, *States and Smugglers: The Ties that Bind and How they Fray*, Mediterranean Dialogue Serries, No. 17, Konrad Adenauer Stiftung, January 2019, p. 6.

(including as a means of quashing protests),[399] whilst Ken Opala reveals patterns of widespread intimidation by both violent criminal gangs and militias on behalf of elements of Kenya's political elite ahead of elections.[400] In turn, this dynamic injects nuance into Biddel's concept of the non-state – state continuum, instead pointing to integrated and overlapping functional sub-networks (spanning across different points of the non-state–state divide) and catering to the needs of a broad range of clients.

5.2 Transport and logistics

The orchestration of clandestine activities is highly contingent on logistical chains as well as accompanying transport solutions. For insurgencies and rebel groups, this typically includes the ability to transport fighters and weaponry within the context of sustained armed campaigns. Meanwhile, logistical solutions, including transnational supply chains, are at the heart of organised criminal business models – constituting the means of bringing illicit goods to market and, therefore, of turning a profit. Perhaps unsurprisingly, an established body of literature points to the extent to which global connectivity and advancements in trade, logistics and transportation support the conduct of operations, increase the geographic reach and of scale activities and, ultimately, enable the projection of power. Observers such as Phil Williams,[401] Rajen Harshe,[402] John Murphy,[403] Philip Cerny,[404] and John McFarlane[405] have thus highlighted the extent to which connectivity has in one way or another catalysed the 'trans-nationalisation' of threats such as crime and terrorism.[406] Although it has been argued that globalisation is in retreat, modern-day non-state organisations (both licit and illicit) clearly continue to reap the benefits from inter-continental travel, communication and supply chain networks as well as accompanying infrastructure.

Even then, case study analysis suggests that the complexity and application of transport and logistics solutions can vary significantly between groups. For example, grassroots and rural insurgencies, rebel movements and smuggling networks may content themselves with relatively simple capabilities such as customised four by four vehicles – typically Toyota pickup truck variants – and motorbikes to meet their day-to-day operational needs. In contexts such as Somalia, Sudan, Afghanistan, Pakistan, Iraq, Syria, Libya, Mali, Chad and Niger, such rudimentary vehicles, which can also be fitted with heavy weaponry, have essentially provided groups with mechanised, 'light cavalry' and logistics capabilities that were once only at the disposal of conventional armies.[407] Other organisations have gone much further, acquiring, as in the case of the Liberation Tigers of Tamil Eelam (LTTE) as well as Mexican and Colombian drug cartels, their own fleets of aircraft and/or maritime capabilities (including, in the case of

[399] L. H. Ong, *Outsourcing Repression: Everyday State Power in Contemporary China*, New York: Oxford Academic (online edition), 2022, pp.16-43.
[400] K. Opala, *Criminal gangs and elections in Kenya*, EU/Enact Report, Issue 37, March 2023.
[401] See P. Williams et al., *Transnational Criminal Organisations and International Security*, Survival, Vol.36, No. 1, March 1994, pp. 96-113.
[402] R. Harshe, *Globalisation and Terrorism*, The Indian Journal of Political Science, Vol. 62, No. 3, 2001, pp.441–45.
[403] J. F. Murphy, *Impact of Terrorism on Globalization and Vice-Versa*, The International Lawyer, Vol. 36, No. 1, 2002, pp. 77-89.
[404] P. G. Cerny, *Terrorism and the New Security Dilemma*, Naval War College Review, Vol. 58, No. 1, Article 2, 2005, p.3.
[405] J. McFarlane, *Transnational Crime: Corruption, Crony Capitalism and Nepotism in the Twenty-First Century*, In P. Larmour and N. Wolanin (eds.), *Corruption and Anti-Corruption*, ANU Press, 2013, pp. 131–45.
[406] See also J. Arquilla and D. Ronfeldt (eds), *In Athena's Camp: Preparing for Conflict in the Information Age*, 1st ed., RAND Corporation, 1997, pp. 315–38.
[407] See also See for example S. C. Tucker (ed), *U.S. Conflicts in the 21st Century: Afghanistan War, Iraq War, and the War on Terror*, Vol. 1 (A-H), Santa Barbara: ABC, 2016, pp. 955-956.

the latter, specially designed submarines).[408] As the modern terrorist hijackings of airliners has shown, transport means can also be exploited for the purposes of committing sensationalist acts of violence.[409]

Both the theoretical and case study literature point to the growing role of independent logistical and professional smuggling networks offering clandestine delivery services to a range of different customers.[410] Moreover, the literature frequently highlights the extent to which these same service providers typically leverage local access – including through relationships with local security actors, cross-border communities and overseas diasporas – in the conduct of their operations.[411] Their knowledge of proven routes, gleaned either through 'dry runs' or insider information (such as in the context of maritime trafficking through major ports) provides them with the means of achieving efficiency and security, whilst reducing business overheads.[412] Furthermore, clandestine groups routinely harness and exploit high-volume trading solutions, hubs and infrastructure as well as economic free-movement zones within the context of their operations. Illustratively, container shipping today provides the primary vehicle for high-volume transatlantic cocaine trafficking, whilst tariff free and/or open border economic zones such as Schengen or the Economic Community of West African States (ECOWAS) allow for largely uninhibited cross-jurisdictional smuggling.[413]

In the case of drug-smuggling networks, multi-customer business approaches using third party providers are evidenced by practices such as the use of dedicated stamps to designate consignments from different producers that are carried as part of the same loads. Indeed, such a practice has been observed within the context of heroin and methamphetamine trafficking across the Indian Ocean and hashish trafficking from Morocco.[414] The evidence also suggests that such service providers may at times constitute a key nexus point between different categories of organisations (such as criminal and insurgent). Illustratively, the often-cited Sahelian case of Mokhtar Belmokhtar, the so-called 'Marlborough Man', shows how influence

[408] See for example N. Manoharan, *Air Tigers' Maiden Attack: Motives and Implications*, Issue Brief, Institute of Peace and Conflict Studies, 2007, pp.1-4; M. Dunigan, D. Hoffmann *et al.*, *Adversary Capabilities in Maritime Irregular Warfare*, In *Characterizing and Exploring the Implications of Maritime Irregular Warfare*, Santa Monica (CA): RAND Corporation, 2012, pp. 69-86; C. Woody, *'El Chapo' Guzman had more airplanes than the biggest airline in Mexico,* Business Insider, May 2016; and B. Ramirez, *Colombian Cartel Tactical Note No. 1: The Evolution of 'Narco-Submarines' Engineering*, Small Wars Journal, https://smallwarsjournal.com/jrnl/art/colombian-cartel-tactical-note-1.

[409] The use of hijacking for the purpose of political messaging began in earnest on July 22, 1968, when members of the Popular Front for the Liberation of Palestine (PFLP) commandeered an Israeli El Al flight traveling from Rome to Tel Aviv. In the following eight years, Palestinian groups would hijack sixteen airplanes, demanding recognition for the Palestinian cause as well as the release of activists imprisoned in Israel.
See D. L. Byman, *The 1967 War and the birth of international terrorism*, Brookings, May 30, 2017, https://www.brookings.edu/blog/markaz/2017/05/30/the-1967-war-and-the-birth-of-international-terrorism/.

[410] J. Bastrup-Birk et al., *Next Generation Organised Crime: Systemic change and the evolving character of transnational organised crime*, Hague Centre for Strategic Studies (HCSS), May 2023, p. 8, https://hcss.nl/wp-content/uploads/2023/05/Next-Generation-Organised-Crime-HCSS-2023-V2.pdf.

[411] See for example, T. Ayalew *et al.*, *Social Embeddedness of Human Smuggling in East Africa: Brokering Ethiopian Migration to Sudan*, African Human Mobility Review, Vol. 4, No. 3, December 2018, pp. 1333-1358.

[412] *Criminal Networks in EU Ports: Risks and challenges for law enforcement*, EUROPOL, March 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal%20networks%20in%20EU%20ports_Public_version.pdf

[413] See for example *Container Control Programme*, United Nations Office on Drugs and Crime (UNODC), https://www.unodc.org/ropan/en/BorderControl/container-control/ccp.html.

[414] See for example: *Analysis of Opiate Stamps Seized in the Indian Ocean: 2017-2021*, Afghan Opiate Trade Project, United Nations Office on Drugs and Crime, 2022, https://www.unodc.org/documents/data-and-analysis/AOTP/Drug_Stamp_Report_Online_1.pdf.

and smuggling expertise gained through cigarette and other commodity smuggling likely paved the way to his jihadist-terrorist linkages.[415] Meanwhile, Nicolas Gosset describes how different smuggling organisations operating in Georgia specialised in drugs, weapons and human trafficking have tended to benefit and draw on the same enabling environments in the conduct of their respective operations across the Caucasus, including by leveraging corrupt relationships and exploiting key transhipment corridors such as the Pankisi Gorge, South Ossetia and Abkhazia.[416]

5.3 Finance and money laundering

The conduct of clandestine activity is fundamentally dependent on funding, which provides the means of purchasing contraband and weapons as well as paying fighters and operatives. In turn, the academic and law enforcement literature highlights the wide plethora of at times complex and often-creative methods and approaches adopted by organisations around the world to raise, transfer and launder funds. These same approaches are steeped in history and tradition. Illustratively, historian Sterling Seagrave describes the ways in which, three thousand years ago, Chinese merchants hid their financial proceeds from rulers by moving these to other jurisdictions.[417] Similarly, early-18th century privateers sold and reinvested their loot via front companies and markets in North America and elsewhere.[418] Opportunities for raising and moving (illicit) proceeds have multiplied in the modern age of global commerce, catalysed by international banking, trade and technology. At the same time, analysis on the extent to which different denominations of clandestine organisations (terrorist, insurgent, criminal, and so on) leverage common financial systems and structures is largely absent in the theoretical debate – partly a product of academic and professional compartmentalisation. For example, James Mittelman and Robert Johnston note that research situating organised crime within the context of an increasingly connected global political economy (the latter of which falls within the purview of political science and economics) is insufficiently captured in the criminological literature.[419] Research and analysis on terrorist financing, including that conducted by the Financial Action Task Force (FATF, the intergovernmental organisation focused on combating illicit financial threats), has similarly tended to be thematically siloed.[420]

Overall, the literature highlights how the financial tools, instruments, and mechanisms at the disposal of clandestine organisations are, to a large extent, only limited by their creativity and access to expertise. Peter Neumann argues that "there are more terrorist organisations, with more money than ever before" despite "blacklists, frozen assets […] and countless regulations designed to prevent terrorist financing."[421] Shima Baradaran *et al* similarly posit that terrorist financial networks have largely been successful in circumventing domestic financial restrictions, including through the creative use of shell companies.[422] In their thorough

[415] *The Central Sahel: A Perfect Sandstorm*, Alternate Forms of Governance, International Crisis Group, June 2015, pp. 15-18.
[416] N. Gosset, *Confronting Threats from the Political-Criminal Nexus in Greater Central Eurasia: Implications for operations and future armed conflicts*, Royal Higher Institute for Defence, Securite & Strategie, No.128, December 2016.
[417] See N. Morris-Cotterill, *Money Laundering*, Foreign Policy, No. 124, May-June 2001, p. 16.
[418] See for example A. Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, The Independent Review, Vol. 11, No. 4, Spring 2007, pp. 565–77.
[419] J. H, Mittelman and R. Johnston, *The Globalization of Organized Crime, the Courtesan State, and the Corruption of Civil Society*, Global Governance, Vol. 5, No. 1, Jan-Mar 1999, pp. 103–26.
[420] See for example *Emerging Terrorist Financing Risks*, Financial Action Task Force (FATF) Report, FATF, Paris, October 2015, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Emerging-Terrorist-Financing-Risks.pdf.coredownload.pdf.
[421] P. R. Neumann, *Don't Follow the Money: The Problem With the War on Terrorist Financing*, Foreign Affairs, Vol. 96, No. 4, July-August 2017, p. 93.
[422] S. Baradaran *et al*., *Funding Terror*, University of Pennsylvania Law Review, Vol. 162, No.3, February 2014, pp. 477-536.

comparative study of terrorism financing techniques, Michael Freeman and Moyara Ruehsen point to spectrum of vehicles and methods used by different organisations to move their funds. These include Informal Value Transfer Systems (IVTS) such as *Hawala* banking, money service businesses, remittance providers, bureaux de change, formal banking services, high value commodities trading and the use of false invoicing.[423] Moreover, observers such as Rodger Shanahan have highlighted the extent to which terrorist groups have harnessed networks of charities and non-governmental organisations – some of these operating behind a humanitarian façade.[424]

Organised crime groups, meanwhile, have arguably leveraged an even greater range of financial mechanisms, resorting *inter alia* to complex and multi-layered offshore money laundering systems and structures aimed at obscuring the origin and movement of funds. A body of literature, in turn, points to the concept of an increasingly interconnected and global 'shadow economy' in which all manner of clandestine organisations, aided by a cadre of so-called 'professional enablers' (white collar specialists such as bankers, tax advisers, notaries and lawyers), are able to circumvent legislation and regulatory frameworks when seeking to move funds across borders.[425] Moreover, technology, including online market spaces and banking services as well as crypto-currencies has arguably exacerbated what Louise Shelly once described as a fundamental transformation in "the very nature of crime itself," all the while threatening "the integrity of the financial system."[426]

These patterns can be further illustrated through the examination of case studies spanning across regions and group denominations. The Lebanese Hezbollah pioneered advanced methods of raising and distributing funds, including in support of its clandestine operations. Over the years, the organisation established tentacles in many industries, a process overseen by a specialist office – the Business Affairs Component (BAC) – situated within Hezbollah's External Security Organisation branch.[427] Hezbollah has also monetised its expertise in money laundering by providing ready-made consultancy services to other clandestine groups. Some of its most profitable ventures take place far away from its 'home turf', such as in Latin America – a region with a lucrative drugs trade and relatively permissive regulatory environment. Here, Hezbollah-linked businesses offer specialised money laundering solutions to customers in localities such as the 'triple frontier' region where the borders of Paraguay, Argentina and Brazil meet. Illustratively, one small currency exchange house linked to Hezbollah's BAC located in Ciudad del Este, close to the Paraguayan border, reportedly laundered almost US $1.5 million in narcotics revenue in exchange for a healthy commission.[428] The separate case

[423] M. Freeman and M. Ruehesen, *Terrorism Financing Methods: An Overview*, *Perspectives on Terrorism*, Vol. 7, No. 4, August 2013, pp. 5–26
[424] R. Shanahan, *Charities and terrorism: Lessons from the Syrian Crisis*, Lowly Institute Report, March 2018, pp. 2-13.
[425] *Professional Money Laundering,* Financial Action Task Force (FATF), 2018, p.6. The Organisation for Economic Development and Co-Operation (OECD) concluded in one study that the overall size of the shadow economy in some countries amounted to around 20 percent of GDP. Shining Light on the Shadow Economy: Opportunities and Threats, OECD, 2017, https://www.oecd.org/tax/crime/shining-light-on-the-shadow-economy-opportunities-and-threats.pdf; See also L. Medina and F. Schneider, *Shadow Economies Around the World: What Did We Learn Over the Last 20 Years?* International Monetary Fund (IMF) Working Paper No. 2018/017, January 2018.
[426] L. I. Shelly, *Crime and Corruption in the Digital A*ge, Journal of International Affairs, Vol. 51, No. 2, 1998, pp. 605–20.
[427] *Attacking Hezbollah's Financial Network: Policy Options*, Hearing Before the Committee on Foreign Affairs, House of Representatives, Serial No. 115-51, US Government Publishing Office, Washington DC, June 2017, p. 10.
[428] E. Ottolenghi, *Lebanon is Protecting Hezbollah's Cocaine Trade in Latin America*, June 2018, Foreign Policy, https://foreignpolicy.com/2018/06/15/lebanon-is-protecting-hezbollahs-cocaine-and-cash-trade-in-latin-america/.

of Kassim Tajideen, a money launderer who worked on behalf of Hezbollah, is also revealing. According to his indictment, Tajideen, a Lebanese-Belgian citizen, ran a business empire which acted as a particularly effective front for concealing international wire-transfers amongst wider business transactions conducted by corporate entities with (deliberately) bland names such as the International Cross Trade Company (ICTC), Epsilon Trading Fze and Sicam Ltd.[429] On paper, Tajideen ran a family business which, as well as offering shipping solutions, traded in poultry, rice, real estate and diamonds.[430] In reality however, his business accounts were used to launder as much as US $50 million of Hezbollah's funds.[431]

As hinted at above, analysis of money laundering systems reveals the extent to which criminal groups have been adept at harnessing systems that fundamentally intersect with the regulated financial system. Thus, the illicit 'shadow' economy is not entirely 'parallel' or 'separated' from the formal economy but instead often exploits and harnesses 'licit' commercial and financial structures within a global financial system lacking accountability and transparency. Illustratively, the so-called 'Panama Papers' – a large trove of financial records that were leaked from the Panamanian law firm Mossack Fonseca in 2016 – highlighted various uses of offshore structures, trusts and corporate service providers in the movement of illicit funds (the papers generated almost 3,500 named individual and company 'matches' against existing Europol records).[432] To be sure, entities such as shell companies and trusts are relatively easy to set up and offer an effective mechanism through which to mask illicit activity behind a facade of licit business activity. In reality however, these vehicles may amount to little more than a name and an address registered to a building located in an offshore jurisdiction to which hundreds of other businesses are also registered.[433] Shell companies can be easily set up via intermediaries using a range of corporate service providers. They need not have any physical employees or products and can be owned by other corporations, nominee shareholders or directors. Once established, these can also hold bank accounts, own property and control assets.[434]

Also illustrative of this theme was the so called 'Russian Laundromat' affair – a scheme that involved the laundering of over twenty billion US dollars linked to, *inter alia*, Russian oligarchs and criminals. Money was 'loaded' onto accounts associated with shell companies that existed only on paper registered in the UK, New Zealand and Cyprus. The companies were then attributed fake business debts, which were ordered to be paid by a corrupt judge in Moldova.[435] The indebted company would then default on the payment, which would in turn trigger a repayment by a third-party company, which had been deliberately set up as a creditor (or

---

Interestingly, the airport of Ciudad del Este has become a notorious and trans-shipment point for narcotics and contraband consignments.

[429] See *United States of America v. Kassim Tajideen*, District Court for the District of Columbia Indictment 1:17-cr-00046, March 2017.

[430] S. S. Hsu, *Lebanese businessman accused of funding Hezbollah pleads guilty to money laundering*, The Washington Post, December 2018.

[431] ICTC accounts, for example, transferred funds from the UAE to multiple jurisdictions, including the United States. See S. Rubenfeld, *Lebanese Businessman Pleads Guilty to Money Laundering*, The Wall Street Journal, December 2018, https://www.wsj.com/articles/lebanese-businessman-pleads-guilty-to-money-laundering-1544200756.

[432] D. Pegg, *Panama Papers: Europol links 3,500 names to suspected criminals*, The Guardian, December 2016, https://www.theguardian.com/news/2016/dec/01/panama-papers-europol-links-3500-names-to-suspected-criminals.

[433] Financial services amount to as much as two thirds of the economy in the Cayman Islands.

[434] D. Morrisey, *Shells Trusts and Similar Entities in International Money Laundering*, US Immigration and Customs Enforcement, Financial Investigations (Miami).

[435] *The Russian Laundromat Exposed*, Organised Crime and Corruption Reporting Project, March 2017, https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.

guarantor).[436] These funds were then paid into a court-controlled account held by Moldindconbank in Moldova, at which point the money was essentially certified and ready for use. Funds were subsequently either withdrawn or transferred onwards, including through Trasta Komercbanka in Latvia, which offered a gateway into the European Union. At this stage, the funds could be transferred easily into larger banks, including Deutsche Bank and Danske Bank.[437] One of the interesting features of the Laundromat affair is that the vast money laundering scheme effectively amounted to a criminal operation in its own right. Just as in the case of specialist transporters, money launderers have therefore also been able to erect their own complex organisations and networks, carving out a position within the international clandestine system.[438]

Meanwhile, examples of technology within the context of clandestine financial operations abound. The use of cryptocurrencies in the conduct of organised crime gained notoriety within the context of Silk Road, a 'dark web' website through which buyers accessed and purchased drugs and other illicit products via digital crypto payments.[439] Michael McGuire similarly describes how most major online booking services such as, for example, the Uber cab-hailing application and AirBnB property letting service, have been exploited for the purposes of money laundering, whilst similarly shining a light on the exploitation of digital marketplaces and social media platforms such as Instagram, Facebook, eBay and Amazon by tech-savvy criminals.[440] Money can also be transferred via gambling websites: one such approach consists of depositing a large amount of funds into an online betting account, placing a few symbolic bets for the purposes of appearance, and then emptying the entire account.[441] Even then, 'tried and tested', localised methods of laundering funds continue to be widely used by organisations seeking to avoid digital signatures. Various branches of the Italian Mafia, Albanian organised crime groups and Chinese triads have therefore shown a preference for traditional uses of small, cash-rich front businesses such as restaurants, nail salons, petrol stations and hotels, alongside real estate investments and construction projects.[442] In the case of the Italian Mafia, criminal bosses developed strategic financial relationships with wealthy restaurateurs and business owners to meet their laundering needs. One such partnership involved the *Righis*, a family who built a large food enterprise in Rome. The family reportedly offered direct investment access to the *Contini Camorra* mafia clan in exchange for protection, a non-union-aligned workforce and discounted black-market ingredients. [443]

[436] The creditor usually consisted of a Russian company involving Moldovan citizens, which is why the case could be settled in a Moldovan court.
[437] Deutsche Bank was also investigated within the context of a mirror-trading scheme facilitated by the Bank's Moscow headquarters which consisted of a software-enabled automated process that imitated international forex trading behaviours, alongside dummy stock purchases.
See for example M. Chan, *Case Study: Deutsche Bank Money Laundering Scheme*, Seven Pillars Institute for Global Finance and Ethics, April 2017, https://sevenpillarsinstitute.org/case-study-deutsche-bank-money-laundering-scheme/.
[438] See also See also See also V. Sokolov, *From Guns to Briefcases: The Evolution of Russian Organized Crime*, World Policy Journal, Duke University Press, Vol. 21, No. 1, Spring 2004, pp. 68-74.
[439] M.H Maras, *Inside Darknet: The Takedown of Silkroad, Centre for Crime and Justice Studies*, CJM No.98, December 2014, pp. 22-23.
[440] See A. Cuthbertson, *Cyber criminals earn $1.5 trillion through Amazon, Facebook and Instagram exploitation*, The Independent, April 2018.
[441] E. Baker, *How Money Laundering Works in Online Gambling*, Casino.org, July 2019, https://www.casino.org/blog/money-laundering-in-online-casinos/.
[442] M. Gottschalk, *'Where the is Pizza there's the Mafia'*, Foreign Policy, August 2007, https://foreignpolicy.com/2007/08/23/where-there-is-pizza-theres-the-mafia/.
[443] D. Conti, *'Want Some Mafia with your Pizza? How The Mob is Taking Over Rome's Restaurants'*, International Business Times, Feb 2014.

5.4 Communication and propaganda

Clandestine campaigns often hinge on communication and propaganda activity, which constitutes a critical means of promoting ideological narratives, mobilising support, sustaining recruitment and infiltrating territory. In turn, the ways and means of doing so may vary considerably across contexts and theatres. David Galula, for example, once noted that "the insurgent, having no responsibility, is free to use every trick; if necessary, he can lie, cheat [and] exaggerate," also adding that "with no positive policy but with good propaganda, the insurgent may still win."[444] For Christopher Harmon and Randall Bowdish, arguments and ideas advanced by groups may gain rapid traction even when these are not entirely coherent, provided the (political) circumstances are generally favourable to these arguments.[445] Ethan De Mesquita and Eric Dickson go further, connecting propaganda with defined objectives such as provoking reactions (such as repressive policies) from state actors that can subsequently be leveraged to justify the terrorist's cause.[446] Commenting on organised crime, meanwhile, Howard Campbell discusses the concept of 'narco-propaganda' in which organisations utilise a combination of criminal behaviour (including violence), videos, symbols and social and mass media as "quasi-ideological expressions" of political and social power.[447] Certainly, as observers such as Cristina Archetti,[448] Reem Ahmed[449] and Richard Moule *et al*[450] point out, the methods of – and opportunities for – disseminating ideas and concepts to multiple audiences has increased significantly within the modern, digitally connected, world.

The relationship between clandestine groups, the media and communication technology as well as the evolution of propaganda methods can be traced across subsequent generations of revolutionary, guerrilla, criminal and partisan movements. Four days after the start of Russia's February Revolution in 1917, the Petrograd Soviet newspaper issued its first newsletter, *Izvestiia* (or news), which would eventually become the official paper of the Soviet government. The international dimension of the movement became increasingly apparent when Bolshevik-supported revolts erupted across Germany, catalysed by sympathetic Bolshevik foreign correspondents.[451] At the same time, the Bolsheviks experimented with new ways of communicating with the masses, including through formats such as newsreels, pamphlets, posters (a method previously used for the purpose of Great War propaganda) and even so-called 'agit-trains' – decorated trains carrying films and projectors aimed at bringing ideas to the largely uneducated rural population. This approach recognised the power of visual

---

[444] D. Galula, *Counterinsurgency Warfare: Theory and Practice*, p. 11.
[445] C. C. Harmon and R. G. Bowdish, *The Terrorist Argument: Modern Advocacy and Propaganda*. Brookings Institution Press, 2018. pp. 5-18.
[446] E. B. de Mesquita and E. S. Dickson, *The Propaganda of the Deed: Terrorism, Counterterrorism, and Mobilization*, American Journal of Political Science, Vol. 51, No. 2, April 2007, pp. 364-81.
[447] H. Campbell, *Narco-Propaganda in the Mexican 'Drug War': An Anthropological Perspective*, Latin American Perspectives, Vol. 41, No. 2, March 2014, pp. 60-77.
[448] C. Archetti, *Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age*, Perspectives on Terrorism, Vol. 9, No. 1, February 2015, pp. 49-59.
[449] R. Ahmed *Online Radicalisation: Current Debates and State Responses*, Sicherheit Und Frieden (S+F) / Security and Peace 37, No. 2 2019, pp. 87-91.
[450] R. K. Moule, D. C. Pyrooz, and S. H. Decker, *Internet Adoption and online Behaviour Among American Street Gangs: Integrating Gangs and Organizational Theory*, The British Journal of Criminology 54, No. 6, November 2014, pp. 1186-1206.
[451] John Reed and Louise Bryant, two supportive American journalists, later published first-hand accounts of this period, *Ten Days that Shook the World* and *Six Red Months in Russia.* See K. McElvanney*, Reporting the Russian Revolution*, British Library, https://www.bl.uk/russian-revolution/articles/reporting-the-russian-revolution#. For an account of events in Germany, see G.P. Bassler, *The Communist Movement in the German Revolution, 1918-1919 A Problem of Historical Typology?*, Central European History, Vol. 6, No. 3, Published by: Cambridge University Press on behalf of Central European History Society, September 1973, pp. 233-277.

mediums in a society in which cinema was becoming the major form of entertainment.[452] The use of the new formats and products spread, exported around the world by socialist idealogues. By the time of the Spanish Civil War, both cinematographic and printed content was produced at scale as a means of mobilising support for and against the Communists' cause, whilst radio broadcasting was used for the first time in conditions of warfare.[453] The conflict also became an early testing ground for the use of information as a lever of proxy warfare, with foreign powers seeking to shape international attitudes and opinions. Strikingly, the call to arms was answered by over 35,000 foreign volunteer fighters from around the world seeking to join Communist International Brigades from 1936 onwards; a demonstration of the global reach of ideological narratives when combined with new dissemination methods as well as of their potential to mobilise multinational (non-state) support for a political cause.[454]

These developments set the tone for World War II – a conflict that witnessed the widespread production and distribution of propaganda material by partisan groups. Within a month of France's occupation by German troops, organisations such as the Paris-based *Musée de l'Homme*, one of the earliest French Résistance networks, began to be publish and distribute clandestine newspapers. The organisation consisted of eight sub-groups, which conducted activities ranging from intelligence gathering to producing periodicals such as *La Verité Française* and *Valmy*.[455] The network also produced hundreds of thousands of pamphlets carrying anti-fascist slogans, some of which were printed on adhesive paper that could be stuck to buildings. Clearly, the risks associated with such activities were high: the architects and backers of *La Vérité française*, including members of the clergy, were rounded up in November 1941 and many of them executed after the group was infiltrated by a German agent.[456] Nevertheless, the work of organisations such as *Musée de l'Homme* and other partisan and resistance groups involved in anti-Axis propaganda across occupied Europe set a powerful precedent for post-war clandestine movements.

With the press, radio and even cinema having now been harnessed by clandestine organisations to broadcast their messages, the stage was set for the introduction of a new, critical, addition to the publicity arsenal: the television.[457] By the 1950s, television sets were being mass-produced for the public with channels adapting the model of radio broadcasting to bring entertainment and news to viewers around the world. The medium gradually established itself as a key conduit for shaping political opinion and relaying high-publicity events. Dwight Eisenhower's presidential campaign staff, for example, began developing shorter, snappier sound bites that could be more easily relayed by television networks. Also in the United States, organised crime contributed disproportionately to establishing the nexus between television and American culture when slow-talking Tennessee Senator Estes Kefauver chaired a series of televised hearings against the criminal boss Frank Costello, a

[452] R. Taylor, *A Medium for the Masses: Agitation in the Soviet Civil War, Soviet Studies*, Vol. 22, No. 4, April 1971, pp. 562-574.
[453] O.W. Riegal, *Press, Radio, and the Spanish Civil War*, The Public Opinion Quarterly, Vol. 1, No. 1, January 1937, p. 134.
[454] See for example J. Marco and P.P. Anderson, *Legitimacy by Proxy: searching for a usable past through the International Brigades in Spain's post-Franco democracy, 1975-2015*, Journal of Modern European History, 2016.
[455] Named after the French victory over the Austro-Prussian armies in the lead to the proclamation of the French Republic in September 1792.
[456] F. Bourrée, *La Vérité française*, Le réseau dit du Musée de l'Homme, Musée de la Résistance en Ligne: 1940-1945, http://museedelaresistanceenligne.org/expo.php?expo=127&theme=253&stheme=486.
[457] The very first model, initially called 'televisor', was invented in 1926 by John Logie Baird who used makeshift materials that included an old tea chest, scissors and bicycle light lenses in order to transfer a moving image to a screen. See J. Staufenberg, *Who invented the television: five facts you need to know about John Logie Baird*, The Independent, 26 January 2016.

notorious gambling magnate and so-called Mafia 'diplomat.'[458] The hearings, in which cameras famously honed in on Costello's nervous hands, not only demonstrated that reality programming could be as popular as entertainment shows or sports; they also signalled the dawn of modern, televised journalism.[459]

For many observers of international affairs, the watershed moment in the evolution of televised news broadcasting of foreign affairs presented itself in the form of the Vietnam War. Here, evening news reports brought footage of combat, bombing campaigns, casualties, and significant events such as the 1968 North Vietnamese Tet Offensive to viewers from across the world and, most critically, to American living rooms. Indeed, the domestic voting population could now (quite literally) observe its country's foreign policy in action. Whilst the true impact of television on the war remains a matter of debate,[460] this did not stop President Lyndon B. Johnson from complaining that "historians must only guess at the effect that television would have had during earlier conflicts on the future of this Nation."[461] The political establishment was further rocked when CBS Evening News anchor Walter Cronkite, 'the most trusted man in America', declared the war a stalemate in February 1968 (shortly after, Johnson announced that he would not be running for re-election).[462]

Certainly, the potential of the medium to shape the attitudes and perceptions of audiences around the world was not lost on clandestine movements, a trend which became apparent when the Palestinian group Black September took Israeli athletes as hostages during the mass-mediatised 1972 Munich Olympics. Thus began what became known as a so-called symbiotic relationship between terrorists and the mass media – the former seeking out the 'oxygen of publicity' required to fuel their political cause; the latter (at least according to sceptics) benefitting from the sensationalist nature of terrorist incidents when competing for viewer attention. Bruce Hoffman thus argues that "without the media's coverage the act's impact is arguably wasted, remaining narrowly confined to the immediate victim(s) of the attack", and therefore failing to "gain the maximum potential leverage [required] to effect fundamental political change."[463] Indeed, the majority of violent terrorist acts of the last five decades – airplane hijackings, high profile attacks and suicide bombings – have been calibrated towards attracting media attention as a means of striking fear amongst some audiences, whilst attracting support from others.

The ability to both generate content and disseminate messages to different audiences around the world has further increased in the modern age of the internet. Clandestine groups are no longer dependent on the editorial decisions of newspapers or television producers and have a fuller reign over messages and narratives. Thus, in 1998, David Duke, the figurehead of America's white supremacist movement wrote about the internet that it would "facilitate a worldwide revolution of white awareness" as well as offer more direct access to its target

[458] K.J. Frydl, *The Drug Wars in America 1940-1973*, Cambridge University Press, New York, 2013, p. 100.
[459] T. Doherty, *Frank Costello's Hands: Film, television and the Kefauver crime hearings*, Film History, Vol. 10, No. 3, 1998, pp. 359-374.
[460] The argument here is that it was in fact the gradual erosion of consensus and support for the campaign amongst the political elite that shaped its outcome.
See for example D. C. Hallin, *The Media, the War in Vietnam, and Political Support: A Critique of the Thesis of an Oppositional Media*, The Journal of Politics, Vol. 46, No. 1, 1984, pp. 2–24, and J. Achenabach, *Did the news media, led by Walter Cronkite, lose the war in Vietnam?*, The Washington Post, May 25, 2018.
[461] M. Mandelbaum, *Vietnam: The Television War*, *Daedalus*, Vol. 111, No. 4, 1982, pp. 157.
[462] M. Bowden, *When Walter Cronkite Pronounced the War a 'Stalemate'*, New York Times, February 26, 2018.
[463] See A. Spencer, *Lessons Learnt: Terrorism and the Media*, AHRC Public Policy Series No. 4, Arts and Humanities Research Council, March 2012, p. 8.

audiences.[464] New online platforms would indeed be harnessed as a means of conveying ideas and ambitions without having to pass through filters and intermediaries, ensuring, as Bin Laden once remarked, that "people [could] understand that what we are telling them is rational."[465] Illustratively, ISIS produced *Dabiq* – a glossy, online magazine which borrowed from al Qaeda's own production, *Inspire,* which was also available in English. As Robert Bunker and Pamela Bunker posit, the online magazine format offers dual benefits, allowing widespread circulation, whilst at the same time presenting a coherent, carefully edited vision (or party line) and accompanying content "without the distortion found in more interactive forms of online media such as chat rooms and forums".[466] Thus, Alexander Meleagrou-Hitchens and Nick Kaderbhai argue that interactive mediums of online communication may shape the attitudes of clandestine support bases to a greater degree than their ideologues and leaders – a dynamic in which online "accessibility [has] trumped ideological authority."[467]

Similarly, social media has played an increasingly important role both in terms of spreading narratives and as a catalyst for radicalisation, offering a powerful means through which to engage in ideological and identity discourse. It was, for example, harnessed by ISIS to propagate a sense of radical, apocalyptic change amongst its followers, with the aim of fuelling excitement and support for its vision of a new caliphate via viral, online social contagion. Whilst the organisation utilised all available platforms, it developed a particular preference for Twitter (now X), a medium also favoured by the Taliban and President Trump. Twitter's appeal consisted of the ability to disseminate a steady stream of propaganda to followers, whilst tweets often included links to other external media content (which, typically, was also produced by the organisation), thus 'confirming' or strengthening messages.[468] A variation of this approach, in turn, can be observed in far right organisations, who have turned to platforms such as Telegram, Facebook and YouTube to both organise campaigns and circulate 'everyday life' videos aimed at encouraging new membership.[469]

Such methods are also used widely by other types of clandestine organisations, including transnational criminal groups. For example, ethnic Albanian criminal gangs involved in cocaine trafficking have turned to social media for demonstrations of wealth and lifestyle as a means of enhancing their reputation and recruiting younger members. These include *Hellbanianz* grassroots gangs with an active presence in East London whose 'specialty' consists of offering local retail services, primarily via street dealing, to the higher echelons of the Albanian Mafia.[470] The potential for glitz, glamour and wealth associated with *Hellbanianz* membership is advertised quite explicitly and openly on platforms such as Instagram. Here, tattoo-clad members pose with eye-catching Ferraris, Lamborghinis and Rolls Royce Phantoms wearing Rolex watches, designer clothes and jewellery. Group photos, moreover, distinctly emphasise an image of brotherhood and fraternity. Videos routinely focus on the gangs' criminal brand

[464] H. J. Ingram, *Islamic State's English-language magazines, 2014-2017: Trends & implications for CT-CVE strategic communications*, International Centre for Counter-Terrorism Research Paper, March 2018, p. 8.
[465] *Draft of a letter to subordinates* (declassified), Bin Laden's Bookshelf, Office of the Director of National Intelligence, https://www.dni.gov/files/documents/ubl2017/english/Draft%20of%20a%20letter%20to%20subordinates.pdf.
[466] R. J. Bunker and P. L Bunker, pp. 1-2.
[467] A. Meleagrou-Hitchens and N. Kaderbhai, *Research Perspectives on Online Radicalisation: A Literature Review 2006-2016*, International Centre for the Study of Radicalisation (ICSR), King's College London, 2017, p. 9.
[468] *Ibid*, p. 64
[469] See for example K. Ihlebæk *et al.*, *What is the relationship between the far right and the media?*, Centre for Research on Extremism, University of Oslo, September 7, 2020, https://www.sv.uio.no/c-rex/english/groups/compendium/what-is-the-relationship-between-the-far-right-and-the-media.html.
[470] M. Bridge, *Albanian gangsters flaunt drugs and guns on Instagram*, The Times, November 13, 2018.

through hashtag descriptors such as '#gang' and '#killer', whilst showing members smoking cannabis, bragging about cocaine distribution and insulting the police.[471] Trap music clips also remind viewers that the gang is "ready for violence."[472] *Hellbanianz* Instagram followers are almost exclusively made up of young males, explaining the potential impact and appeal of descriptions and comments such as "[I] told her my life's like a movie, you ain't gotta go [to the] cinema."[473]

5.5 (Counter) Intelligence and operational security

Organisations operating in the face of adversity – including sustained attempts by state actors to disrupt their activities – have had to adopt a range of measures aimed at enhancing their operational security and ensuring secrecy. Moreover, the theme of clandestine non-state actor uses of communication technology (see above) also introduces a closely related topic: that of (at times) sophisticated intelligence methods and capabilities as a key operational enabler. Speaking of guerrilla movements, Patricia Hoffman commented that "the primary element [in their] favour is superior intelligence," and that "to evade the adversary's strengths and attack his weaknesses, a guerrilla must know the enemy's disposition and readiness, his movements and intentions, his proclivities and patterns," whilst at the same time keeping "his own intentions hidden from the adversary."[474] John Gentry expands on the concept, suggesting that clandestine non-state actors harness intelligence for the purposes of planning attacks, protecting themselves from (state actor) penetration, ensuring their survival and shaping the overall operating environment.[475] Reflecting on these dynamics, David Strachan-Morris posits that such actors need to be understood as intelligence actors in their own right.[476] Turning to terrorist actors specifically, Mohammad Iqbal describes the ways in which groups have adapted to and learned from state intelligence methods, at times 'leapfrogging' them through their ability to implement new measures at a faster pace.[477] Moreover, a smaller but growing body of analysis points to criminal uses of (counter) intelligence methods by organised crime groups, including for the purposes of anonymisation (recent analysis also highlights how artificial intelligence is also being leveraged for this purpose).[478]

Clandestine reconnaissance and intelligence-gathering methods, in turn, have been employed consistently throughout history. Native American warriors employed smoke signals to warn of impending dangers and rally support from other tribes, whilst armies dating back to at least the campaigns of Genghis Khan used dispatch riders and homing pigeons to relay orders and intelligence between field units.[479] During the American Revolutionary War, informants

---

[471] Analysis of *Hellbanianz* Instagram accounts and followers, January 2021.
[472] M. Townsend, *Kings of cocaine: how the Albanian mafia seized control of the UK drugs trade*, The Guardian, January 13, 2019, https://www.theguardian.com/world/2019/jan/13/kings-of-cocaine-albanian-mafia-uk-drugs-crime.
[473] *Hellbanianz* Instagram analysis, January 2021.
[474] P. D. Hoffman, *Seeking Shadows in the Sky: The Strategy of Air Guerrilla Warfare*, Air University Press, June 2000, p. 22, https://www.jstor.org/stable/pdf/resrep13758.8.pdf.
[475] J. A. Gentry, *Toward a Theory of Non-State Actors' Intelligence*, Intelligence and National Security, Vol. 31, Issue 4, 2015, pp. 465-489.
[476] D. Strachan-Morris, *Developing theory on the use of intelligence by non-state actors: five case studies on insurgent intelligence*, Intelligence and National Security, Vol. 34, September 2019, pp. 980-984.
[477] M. N. F. Iqbal, *Leapfrogging: Terrorists and State Actors*, Small Wars Journal, August 2017, https://smallwarsjournal.com/jrnl/art/leapfrogging-terrorists-and-state-actors.
[478] See for example V. Ciancaglini et al., *Malicious Uses and Abuses of Artificial Intelligence*, Trend Micro Research, December 2021, https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence.
[479] These were reflected *inter alia* in the British Navy's Permanent Fighting Instructions of 1691. See J. J. Tritten and L. Donolo, *The Navies of the United States, Great Britain, France, Italy and Spain*, A Doctrine Reader, Newport Papers (No.9), Naval War College, December 1995, pp. 4-6.

working for both the British and American colonists used unofficial messengers who operated outside the colonial postal system. At the time of the Peninsular War of 1807-1814, the Duke of Wellington leveraged an entire ring of non-state agents who supplied vital intelligence on the movements, intentions and morale of French reinforcements.[480] Intelligence-gathering activity reached a historical climax during World War II, during which entire networks of local informants and operatives moved across borders and occupied zones to both report on enemy movements and conduct subversive activities such as sabotage.[481] Nancy Wake, a British agent who worked with the French Resistance to help hundreds of allied soldiers escape occupied France, believed that her most useful contribution to the war effort consisted of cycling five hundred kilometres to replace the codes of her wireless operator.[482] Traditional intelligence gathering and target reconnoitring techniques continued to be utilised widely by clandestine organisations in the second half of the 20th Century. During the Vietnam War, for example, the Viet Cong employed local militia groups to provide information on events and enemy movements in and around their villages,[483] whilst the Revolutionary Armed Forces of Colombia (FARC) surveyed potential targets prior to kidnappings and collected human counterintelligence insights from corrupt government officials.[484] Taking this trend even further, the Mexican Las Zetas and Los Caballeros Templarios (Knights Templar) cartels enlisted former Special Forces soldiers trained in both intelligence gathering and interrogation.[485]

Today, the act of collecting useful information and identifying targets is simplified by modern technology. Operatives engaging in hostile reconnaissance can research potential operations via commercially available online maps and satellite imagery. They can also photograph, film, monitor and share information on targets and enemy movements using little more than their smartphones.[486] Air assets such as commercially available drones, meanwhile, have been

---

[480] For a detailed account of Wellington's intelligence network see H. J. Davies' *Spying for Wellington: British Military Intelligence in the Peninsular War*, University of Oklahoma Press, Norman, 2018.

[481] The US Special Operations Research Office highlighted the seminal role of such agents in reporting on transport and communication links, but also in "conducting strategic acts of sabotage and encouraging the populace to engage in general acts of destruction" as well as to "commit people more firmly to the cause." A. R. Mulner *et al.*, *Undergrounds in Insurgent, Revolutionary and Resistance Warfare, Special Operations Research Office*, American University, Washington D.C, November 1963, pp. 30-31, Approved for release in September 1999. Available online at: https://www.cia.gov/library/readingroom/docs/CIA-RDP78-03581R000200100001-5.pdf.

[482] K. Willsher, *Farewell to Nancy Wake, the White Mouse who ran rings around the Nazis*, The Guardian, August 2011.

[483] R. R. Leonhard*, Undergrounds in Insurgent, Revolutionary and Resistance Warfare*, United States Army Special Operations Command (USASOC), Second Edition, Fort Bragg, NC, 2013, p.48.

[484] See R. Vargas, *The Revolutionary Armed Forces of Colombia (FARC) and the Illicit Drug Trade*, Transnational Institute Policy Briefing, June 1999, available online at: https://www.tni.org/en/publication/the-revolutionary-armed-forces-of-colombia-farc-and-the-illicit-drug-trade.

[485] F. Ernst, '*The training stays with you': the elite Mexican soldiers recruited by cartels*, The Guardian, February 2018, available online at: https://www.theguardian.com/world/2018/feb/10/mexico-drug-cartels-soldiers-military.

[486] Moreover, photographs taken with high-end Digital Single Lens Reflex cameras and telephoto lenses are easily uploaded and shared using only a Secure Digital (SD) card and laptop. These can be geotagged and integrated alongside other aids as part of the planning processes. Such methods are also increasingly and routinely being socialised, and not always in a covert manner. Although often exaggerated, television series and films continuously offer insights into some of the techniques and tools used by criminal and terrorist actors as part of their preparations. See for example: *The use of the Internet for terrorist purposes*, United Nations for Drugs and Crime, New York, 2012, pp.8-10, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, and T. Harding, *'Terrorists use Google Maps to Hit UK Troops'*, The Telegraph, January 2007, available online at: https://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

harnessed by groups such as ISIS for the purposes of both aerial surveillance and as a weaponised means of delivering explosive payloads.[487] For organised crime groups, technology-enabled intelligence gathering may range from researching prospective markets – such as the price of commodities and contraband in any given location – to investigating border crossing points and/or more discrete disembarkation areas along coastlines. Modern connectivity also allows such organisations to identify, contact and recruit local 'insider' informants such as airport baggage handlers and dockworkers through company websites and social media who can, in turn, document and report on security measures and/or partake in criminal activities. More widely, insurgents, terrorists and criminals have demonstrated the value of both battlefield-specific communications capabilities – such as tactical Very High Frequency (VHF) radio sets – and more readily available mobile phones to coordinate tactical activity on the ground.[488] VHF radios, satellite phones and other 'off the shelf' solutions such as Global Positioning Systems (GPS) also constitute useful tools for organised crime groups seeking to arrange the movement of illicit goods, particularly in more remote areas with limited coverage.[489] This might include cross-decking drug consignments between vessels on the high seas, organising rendezvous and handovers in the desert, or dropping off contraband along rugged coastlines under the cover of darkness. Furthermore, groups can choose between readily downloadable encrypted mobile communication applications with self-destructing, 'secret chat' functions and custom-built secure devices for added operational protection.[490]

5.6 Internal and outsourced expertise and know-how

Taken together, many of the above levers of power and domains of activity point to the cross-cutting and growing importance of expertise and know-how as a clandestine 'force multiplier.' The specialist skills required within the context of setting up complex money laundering operations or developing offensive capabilities, a task described by Gary Ackerman as "complex engineering," have, as we have seen, catalysed specialised sub-networks and nodes characterised by high levels of professionalism and technical knowledge.[491] Indeed, the previously described case of IED manufacturing hints at the importance of niche skills within the context of planning and conducting more advanced asymmetric or clandestine operations. Whilst it is true that bomb-making technology has migrated in recent years, forensic and fingerprint evidence gathered as part of counter-IED efforts in Iraq and elsewhere have demonstrated that even here, multiple devices can be traced to the same manufacturer.[492]

---

[487] This includes the use of the Chinese Skywalker Technologies-manufactured X8 drone, with its impressive two metre wingspan and high-definition camera. See C. Clover and E. Feng, *ISIS use of hobby drones as weapons tests Chinese makers, The Financial Times*, December 2017.

[488] ISIS fighters in Iraq were able to go one step beyond this when they captured US-made encrypted radio systems from the Iraqi army during their offensive in 2014.

[489] *Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries*, United Nations Office on Drugs and Crime, September 2002, p. 109.

[490] Illustratively, a large pan-European law enforcement operation conducted in 2020 uncovered the widespread use of EncroChat, an encrypted phone network consisting of a secure digital communication tool loaded onto ordinary smartphones, by criminal groups.
Dismantling of an Encrypted Network Sends Shockwaves through Organised Crime Groups Across Europe, Europol/Eurojust Joint Press Release, 2 July 2020,
https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted.
In a more traditional variation on this theme, SMS payment reference codes and receipts are at times issued by Hawaladar bankers as a means of validating and securing payments. See *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, Financial Action Task Force, October 2013, p. 29.

[491] G. A. Ackerman, *Designing Danger: Complex Engineering by Violent Non-State Actors: Introduction to Special Issue*, Journal of Strategic Security, Vol. 9, No. 1, Spring 2016, pp. 1-11.

[492] See for example: C. Dillow, *To Catch a Bombmaker*, Popular Science, September 2015, available online at: https://www.popsci.com/to-catch-bomb-maker.

ISIS, moreover, established a model where explosive devices were made at scale in specifically designed mobile factories built for mass production. Although still requiring overall technical supervision and expertise, these were assembled by a workforce that included mechanics whose job consisted of making metal screws and bomb parts alongside an assembly crew staffed by forced labourers.[493] Some organisations, such as al Qaeda, have traded on their expertise, offering training and know-how to localised franchises around the world.[494] Again, knowledge ranging from the selection of weapon systems to tactical manoeuvring can often be traced back to state actors. Illustratively, Mujahideen Ahmed Shah Massoud and Gulbuddin Hekmatyar both received such training from the Pakistani intelligence service (ISI), whilst Iran's provision of support to proxies such as Hezbollah has gone far beyond the simple provision of IED know-how to include missiles.

Niche skills and expertise arguably play an even more critical role within the context of transnational organised crime networks. As previously argued, illicit enterprises increasingly rely on a web of specialist service providers and sectors who interact and trade with one another based on their everyday business needs and respective 'value added' skills. This means that each specialised sector or provider typically has its own unique set of skills that it can monetise as part of international production processes or supply-chains. The narcotics business, for example, is reliant on laboratory technicians and chemists to produce commodities such as heroin, cocaine and synthetic drugs. In the case of the heroin trade, this includes individuals who have the knowledge and expertise to first turn wet opium extracted from poppies into morphine base through a reduction process involving hot water, lime and ammonium chloride and, subsequently, convert the morphine into heroin.[495] Whilst heroin can technically be produced through crude means and field laboratories, specialist know-how is particularly important in order to produce higher-purity variations of the drug intended for high-paying customers in Western markets. Such a process might involve more sophisticated equipment such as litmus paper, stainless steel pots, propane gas ovens, Bunsen burners, vacuum pumps and electric drying ovens.[496] Moreover, the need for specific precursor chemicals such as Acetic Anhydride has effectively resulted in the creation of dedicated precursor supply chains comprising specialised smuggling networks and front organisations such as pharmaceutical supply companies.[497]

The need for – and leveraging of - specialist services and products is also apparent within the context of professional counterfeiters. Counterfeiting is arguably one of the oldest forms of criminal services alongside smuggling. Historical accounts, for example, point to the use of fake official documents in the Roman empire – a phenomenon that triggered a stern response by way of the highly punitive law of Lucius Cornelius Sulla.[498] In 15th Century Japan, Honoi merchants trading on the routes connecting Kyoto to north-eastern Japan sought to

[493] E. Solomon and S. Jones, *Isis' bomb-making expertise leaves lethal legacy*, The Financial Times, October 2016.
[494] B. Lia, *Al-Qaida's Appeal: Understanding its Unique Selling Points*, Perspectives on Terrorism, Vol. 2, No. 8, Terrorism Research Initiative, University of Leiden, 2008, available online at: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/44/html.
[495] The latter synthesis involves a process that requires around twelve to fourteen hours to complete as well as a number of precursor chemicals, chief amongst which is Acetic Anhydride.
See U. Zerell *et a*l., *Documentation of a heroin manufacturing process in Afghanistan*, Bulletin on Narcotics, Volume LVII, No. 1&2, 2005, pp. 11-31.
[496] *Opium Poppy Cultivation and Heroin Processing in Southeast Asia*, Drug Enforcement Administration Office of Intelligence, U.S. Department of Justice, September 1992, p. 15.
[497] See for example *Financial flows linked to the production and trafficking of Afghan Opiates*, Financial Action Task Force, Report, June 2014, pp. 38-39
[498] D. Potolinca *et al.*, *The Study of Documents Counterfeit Procedures by Analyzing the Security Elements*, International Journal of Criminal Investigation, Vol. 2, Issue 3, p. 221.

consolidate their rights and prerogative as traders by forging imperial decrees.[499] During World War II, counterfeit documents – passports, work passes, firearm licenses and travel permits – were manufactured at an almost industrial scale by the Allies in specialised facilities for partisans and special operations agents as well as for the purpose of counter-German propaganda.[500] Forgers and counterfeiters, however, have come into their own in the modern age, servicing high levels of demand on the black market and aided by technological aids such as readily-available editing software and printers. Here, key geographic centres stand out in the international illicit services market. Illustratively, Bangkok's Little Arabia district may well have established itself as a global hub for fake passports with Australian, British and American versions fetching up to US $2,500.[501] Whilst particularly popular with irregular migrants, fake identity documents are also a critical enabler for both terrorists and organised criminals as well as for money laundering activity.

Returning to a familiar theme, the migration of expertise and knowledge between organisations has clearly been catalysed by globalisation, international trade and the proliferation of modern communication technologies. Indeed, knowledge has become a prized commodity that can be traded or purchased in its own right on the global black market. Around the same time as al Qaeda was sending emissaries and trainers to upskill different international franchises in the use of terrorist tactics, the Pakistani Nuclear scientist Abdul Qadeer (aka 'AQ') Khan was proliferating uranium enrichment technology to Iran, North Korea and Libya, sparking fears within the international community that nuclear capabilities and knowledge could eventually be acquired by terrorist organisations.[502] The purchase of knowledge, including through the employment of specialist consultants, is also apparent within the context of the global criminal economy. Illustratively, drug trafficking organisations in the Netherlands have at different times sought to acquire cocaine-processing expertise from Colombian groups,[503] whilst Russian and Ukrainian cybercrime specialists have effectively become the go-to providers for malware code and cyberweapons. Taken together therefore, these various dynamics point to an increasingly connected ecosystem in which all manner of organisation can source expert services from specialists as part of an integrated and highly lucrative marketplace.

5.7 Conclusion

This chapter outlined the wide range of levers available to clandestine non-state actor seeking to project power, including transnationally. Speaking to this thesis' third hypothesis and drawing on both theoretical sources and empirical analysis, it showed how these actors have shown a propensity to both develop and combine capabilities and instruments in a way that is, at least conceptually, not too dissimilar to the approaches adopted by states, albeit typically at a smaller scale. This investigation also built on the previous examination of clandestine organisational structures and operating models, not least because specific functions and

[499] H. Tonomura, *Forging the Past: Medieval Counterfeit Documents*, Monumenta Nipponica, Vol.40, No.1, Sophia University, Spring 1985, pp. 69-70.
[500] One of the more imaginative examples was a fake Hitler passport doctored to make him look Jewish and carrying a Palestinian visa. "Small moustache," it noted, under the 'distinguishing features' section. See '*Adolphe Hitler's Fake Passport*', The National Archives, available online at: https://www.nationalarchives.gov.uk/museum/item.asp?item_id=46.
[501] S. Berger, *Welcome to Bangkok, the capital of forgery*, The Telegraph, August 2005, available online at: https://www.telegraph.co.uk/news/worldnews/asia/thailand/1497014/Welcome-to-Bangkok-the-capital-of-forgery.html.
[502] See for example C. Collins and D. Frantz, T*he Long Shadow of A.Q. Khan: How One Scientist Helped the World Go Nuclear, Foreign Affairs*, January 2018.
[503] See for example D. Zaitch, *Trafficking Cocaine: Colombian Drug Entrepreneurs in the Netherlands*, Studies of Organised Crime, Kluwer Law International, The Hague, 2002, p. 290 and J. M. Bunck and M. R. Fowler, *Bribes, Bullets and Intimidation: Drug Trafficking and the Law in Central America*, Pennsylvania State University Press, 2012, p. 27.

capabilities often call for a degree of specialisation and professionalization, including with respect to the development of offensive weaponry, transport solutions, intelligence-gathering and financial-transfer systems. Of course, such specialisation can also be outsourced or delegated to external third-party providers and professional enablers, some of whom may work concurrently for a number of different clandestine organisations. This pattern introduces further granularity within the context of the thesis' first hypothesis, specifically with respect to the character of inter-non-state actor partnerships. Cross-network interlinkages, this chapter has argued, are on the rise in the digital era, with online platforms, tools and mediums offering distinct advantages regarding the acquisition of capabilities, long-distance coordination of clandestine activities and the dissemination of propaganda and strategic communications content. More broadly, the analysis provided over the course of the last three chapters has highlighted how clandestine non-state actors, whilst smaller and weaker than states in the conventional sense, have other tools at their disposal, including flexibly and adaptability, arguably reflecting what Foucault once described as the 'pluralist' nature of power.[504] Still, the various dynamics captured within the above framework require further empirical validation, which this thesis will now seek to achieve by applying the framework to the detailed examination of three groups operating in significantly different contexts.

[504] See H. T. Miller, Governmentality, *Pluralism, and Deconstruction*, Administrative Theory & Praxis, Vol.30, No.3, Taylor & Francis, pp. 363-368; and K. J. Heller, *Power, Subjectification and Resistance in Foucault*, SubStance, Vol. 25, No. 1, Issue 79, Johns Hopkins University Press ,1996, pp. 78-110.