Counterintelligence and Escalation from Hybrid to Total War in the Russo-Ukrainian Conflict 2014-2024

Professor Philip H.J. Davies

Director, Brunel Centre for Intelligence and Security Studies (BCISS)

Brunel University

Uxbridge, Middlesex

UK, UB8 3PH

E: Philip.davies@brunel.ac.uk

T: +44 (0)7790 496 346

M: +44 (0)7790 496 346

Abstract

This article examines certain counterintelligence (CI) aspects of the on-going conflict between Russia and Ukraine since 2014 in terms of key conceptual problems in current western CI concepts, doctrine and processes. It examines not only the CI threat to Ukraine during the Donbas 'frozen war' and 2022 invasion from the traditional CI triad of espionage, sabotage and subversion but also from Russian intelligence, surveillance and reconnaissance (ISR) capabilities and activities supporting both irregular and regular combatants. The article concludes that a UK and allied approach to CI shaped by a two-decade security focus on counterterrorism and counterinsurgency may not be for purpose in a contemporary strategic environment characterized by a persistent and escalating threat from strategic peers and state-supported hybrid conflict.

Keywords

Russia, Ukraine, Counterintelligence, SBU, FSB, FRU, Russo-Ukraine War

Author Bio

Professor Philip H.J. Davies is Professor of Intelligence Studies at Brunel University, London where he is also Director of the Brunel Centre for Intelligence and Security Studies (BCISS). Professor Davies specializes in social science, policy and comparative approaches to national and defence intelligence institutions. He is the author, *inter alia,* of *MI6 and the Machinery of Spying* (2004), *Intelligence and Government in Britain and the United States* (2012) and co-editor of *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (2013). Besides working extensively on the UK and US intelligence communities he has also published on the intelligence systems of Canada, Malaysia , India and Russia. In 2010-11 he was one of the authors of the third edition of the UK joint military intelligence doctrine and the first edition of the keystone doctrine on 'Understanding' for operational commanders. Most recently, he was on the drafting team of the fourth edition of the UK joint intelligence doctrine (issued in 2024) and has been conducting research on defence and military counterintelligence.

ORCID: 0000-0003-3820-8862

Introduction

In 1946, the British War Office *Manual of Military Intelligence* counterintelligence pamphlet opened with the blunt but lucid assertion that: 'The object of counterintelligence is to destroy the effectiveness of the enemy intelligence organization.'[1] While counterintelligence (CI) features as a standard entry in almost every study of intelligence and constitutes one of Roy Godson's influential 'elements of intelligence'[2] it has received far less academic discussion than the other elements of covert collection, covert action and intelligence analysis. If intelligence is sometimes portrayed as a handmaiden to policy, counterintelligence tends to be treated as a handmaiden to intelligence. In its conventional use, even amongst professionals and entirely accomplished scholars of intelligence, CI tends to be treated simplistically as 'catching spies' or 'hunting moles'. [3] But in fact, CI is a much more nuanced matter, with significant divisions of opinion, divergences in professional practice and, at times, even profoundly different basic mandates for the organisations that are nominally engaged in CI. Indeed, CI is perceived differently and conducted differently not only between different levels and branches of government, but sometimes even *within* different parts of the same organization.

Many of the dilemmas, disputes and schisms within CI are, moreover, quite fundamental ascribing to it very different roles, remits, and responsibilities. As a result, while most CI practitioners might heartily agree with the post-war British Army, no one can otherwise quite agree what 'destroying the effectiveness of the enemy intelligence organization' entails. Nonetheless, the CI community (broadly understood) largely sees itself as muddling through barring intermittent (and sometimes more than intermittent) jurisdictional disputes, persistent but usually manageable miscommunications and misunderstandings, and the occasional and often embarrassing lapses in providing CI capabilities, products and services. But, in fact, CI theory, doctrine, policy and sometimes practice are deeply troubled amongst the UK and her allies, whether NATO, Five Eyes or further flung alliances and coalitions around the globe.[4]

The on-going and devastating war in Ukraine has, more than many conflicts in recent history, been seen as especially and especially *visibly* a conflict informed and shaped by intelligence, and especially recent innovations and transformations thereof that have emerged over the last couple of decades. With intelligence displaying such significance one might reasonably expect that CI should also have a similar level of importance and impact in the conflict, whether in terms of its effective delivery or ill-considered neglect. And, indeed, there have been eye-catching and very public CI moments such as a surge of investigations and arrests of senior Ukrainian national security officials for treason on behalf of Russia that began shortly after the war, and the wholesale expulsion of Russian intelligence officers working under diplomatic cover from their embassies around the world. But these moments of espionage and counter-espionage drama are not, in fact, the most important issues to emerge from the CI dimension of the Russo-Ukrainian War.

The Russo-Ukrainian war drives directly into some of the most important fracture lines in current Western CI thought and practice. This arises in a large part from its backstory of the collapse of the Union of Soviet Socialist Republics (USSR) in 1991. But equally important is the conflict's escalation from a case-in-point of contemporary state-backed hybrid or 'full spectrum' conflict to one of (at least for Ukraine) total war. For two decades after the September 11, 2001 terrorist attacks on the United States, Western national security institutions focused almost exclusively on what John Gentry has referred to as 'violent non-state actors' (VNSAs) in a succession of counter-terrorism (CT) and counter-insurgency (COIN) campaigns.[5] For all of their assiduous efforts and often formidable competence at engaging in operational and tactical intelligence, however, VNSAs cannot command the range of capital-intensive, often highly technical intelligence collection and exploitation capabilities available to state-level strategic peers. The Russo-Ukrainian conflict, however, has embodied the worst of both symmetrical and asymmetrical conflict. Russia has invested heavily in orchestrating and resourcing VNSAs amongst Russophile and ethnic Russian communities in the flank states of the former USSR while also supporting them with state-level intelligence, surveillance and reconnaissance (ISR) assets. This characterized both the 2014 seizure of the Crimea and subsequent so-called 'frozen war' in the Donets Basin (Donbas) area of the Donetsk and Luhansk administrative regions or *oblast*s. Russia then brought the full weight of its national and military intelligence apparatus to bear on Ukraine with the all-out invasion in 2022.

The Russian intelligence threat that has manifested in the Ukraine conflict is, therefore, precisely what UK and allied counterintelligence have *not* been prepared to deal with for a generation. Terrorists, insurgents and other VNSAs may not have gone away, and really they never do. But the state-level threat also did not go away either during the so-called 'war on terrorism' and it is, in fact, likely to dominate the coming decades and very probably for significantly longer. And the most important lesson to draw from the CI experience in the current war is that a counterintelligence

model suited to CT and COIN is almost entirely ill prepared to deal with that new strategic environment.

A Splintered Specialism

It will come as a surprise to no one in a field like intelligence where no one can quite agree what 'intelligence' itself means that the core concepts and remit of *counter*intelligence are also chronically subject to contention, schisms, factions and disputes. There are, to be sure, areas of some stability in the field. By and large, CI has had a more or less stable core remit, since at least the 1920s, consisting of three main fields of endeavour: counter-espionage (CE), counter-sabotage and counter-subversion. Typically, stand-alone counter-sabotage has been regarded chiefly as a wartime concern and largely subsumed by protective security policy in peacetime, although that distinction is far less clear in a hybrid war context. At the level of national intelligence institutions, counter-subversion became a much less tenable mandate after the social changes of the 1960s and successive revelations about security investigations of what were perceived as social movements of legitimate dissent. Successive allegations and consequent furores amongst the media and political classes rendered counter-subversion so reputationally damaging that the intelligence communities of the Anglophone democracies could not drop the function fast enough as soon as the Cold War ended.[6] In one of many divergences from national intelligence practice, however, counter-subversion has persisted relatively unchallenged in military counterintelligence doctrine[7], perhaps due to the much less ideologically ambiguous and more professionally disciplined environment of the armed services and their regulations.

That core mandate has, however, somewhat fuzzy boundaries. In some cases, the CI remit includes assassination[8], which is not unreasonable if one views assassination as a variation on or sub-category of sabotage. For reasons that, as yet, remain somewhat unclear from the 1970s many versions of the CI remit have included counter-terrorism. This appears to have arisen at least partly from viewing terrorists and insurgents as non-state purveyors of sabotage and subversion[9] and a Cold War perception that prevailed until the early 1980s that they were also either proxies for, or at least resourced and heavily influenced by, state actors chiefly from the erstwhile Communist bloc.[10] Indeed, in 1999 this prompted a slightly and atypically intemperate push-back from UK joint doctrine writers as drifting too far from the central military CI mission of comprehensively countering adversary intelligence capabilities and activities in the battlespace.[11] Most recently and slightly bizarrely, chiefly in the context of COIN campaigns in Afghanistan and Iraq, since 2015 NATO CI doctrine has also added countering organized crime to CI's responsibilities.[12] The result has been in some respects, a seemingly syncretic CI mission creep away from 'destroying the effectiveness of the enemy's intelligence organisation'.[13]

Even within that core mandate there have been chronic points of dissent and friction. Arguably, the most visible of these have been basic cross-jurisdictional tensions over the degree to which it is an intelligence or law enforcement function and should be dominated by the priorities of investigation and enforcement or penetration and what it is currently fashionable to refer to as 'information advantage'. [14] And, as Arthur Zuehlke observed in a pithy, thorough, seminal and still applicable concise discussion of CI principles 1980, it has also been dogged by a tension between the priorities of passive defensive security measures and policy and offensive penetration of adversary intelligence organizations. Zuehlke argues that this latter is something of a false dichotomy because of a fundamental interdependence of the two functions and hence was, in his opinion, something of

a dead issue by the time he was writing.[15] As we shall see shortly, this is far from being the case, especially with regards to *military* counterintelligence.

But there are a number of, even more fundamental, tensions that are especially relevant to the Ukraine conflict.

Counter-What Exactly?

As far back as 1904, David Henderson warned in his instructions to military intelligence personnel that: 'It is safe to estimate that the efforts of the enemy to gain information will be at least as energetic as our own, and that he will neglect none of the various methods which are usually followed.'[16] At the turn of the Twentieth Century this was almost entirely confined to enemy intelligence personnel engaged in clandestine reconnaissance and surveillance or running human sources close to and across the front lines. Not a decade later, the First World War heralded in a sea change in intelligence with the explosive development of technical intelligence collection methods such as the interception of landline and wireless telecommunications and overhead photographic reconnaissance. This rapid evolution of technical collection systems and platforms would create a profound conceptual schism regarding what counterintelligence is supposed to counter.

As noted in the introduction, CI is often perceived simply as 'catching spies'. On the other hand, were we to speak of *friendly* offensive intelligence collection activities against a rival, adversary or enemy we would not equate 'intelligence' merely with HUMINT. Indeed, it is virtually axiomatic that intelligence should seek to be an *all source* enterprise as far as feasible and appropriate. Given this premise, it seems oddly constrictive or selective to restrict the countering of rival, adversary or enemy intelligence to opposing solely their HUMINT efforts. In 1980, Arthur Zuehlke voiced a significant dissent regarding this conventional view of CI. He warned that while most approaches to counterintelligence tended to be exclusively concerned with counter-HUMINT, actual hostile intelligence collection activities covered the full gamut of collection disciplines, overt and covert. Counterintelligence, he argued, needed to be seen as 'multi-disciplinary'[17], concerned as much with adversary signals, imagery and open source intelligence as with countering HUMINT and other activities delivered by HUMINT agencies, like sabotage and subversion.

The concept of 'multidisciplinary counterintelligence' (MDCI) would make its way into wider US intelligence thinking as a standard term of art in the 1990s. Almost immediately there appears to have been some disagreement as to whether it included counter-HUMINT or referred purely to countering technical intelligence collection disciplines as a technical counterpart to 'counterespionage' against human threat vectors. But, on the whole the weight, of official opinion was to include human as well as technical intelligence threats under the concept.[18] Indeed, when Britain's joint doctrine writers complained in 1999 about the inclusion of terrorism in NATO CI doctrine and a general overemphasis on 'human factors', their preferred concept of CI against the full range of human and technical disciplines incorporated into the enemy's 'intelligence, surveillance, target acquisition and reconnaissance' (ISTAR) efforts.[19] ISTAR at the time was the UK counterpart to the US-originated notion of 'intelligence, surveillance and reconnaissance' (ISR). The latter has since become the preferred term of art across the NATO and 'Five Eye' (FVEYE) alliances.[20]

Indeed, MDCI has a very specific significance to defence and military operations because so many of the ISR systems and capabilities deployed into the battlespace *are* technical collection systems. Prior to 9/11, there was an explicit perception on both sides of the Atlantic that the fundamental task of CI in military operations was an MDCI mission focused on counter-ISR (or counter-ISTAR). In the wake of 9/11, however, the so-called 'war on terrorism' was conducted against terrorists and

insurgents who were only minimally ISR enabled, and so the emphasis shifted away from MDCI to purely human threat vectors. The Russo-Ukraine conflict, however, has been characterised since its earliest stages by Russophile insurgents and partisans supported by Russia's state-level ISR capabilities.

A Tale of Two Securities

Arthur Zuehlke, as noted above, suggested in 1980 that the tension between security and offensive counterintelligence was largely a settled matter. At the national CI level this might appear plausible in principle albeit unlikely in practice. As far as defence and military operations are concerned, the dilemma is very far from being settled. Indeed, it is arguably also far less tractable. This is because military CI is chronically caught in a tug of war between two entirely different notions of 'security'. Those two notions of security are protective security , usually framed in the military context as 'force protection' (FP), and operations security (OPSEC). FP is essentially about preventing compromise to military personnel, equipment and facilities from enemy espionage, sabotage and subversion (and also, depending on doctrine, terrorism and organized crime). OPSEC, however, is essentially about ensuring freedom of action, or 'freedom to operate', by denying the enemy both advance and current knowledge of those operations that would help them prevent, pre-empt or interdict friendly operations. From the OPSEC point of view, CI is constantly in danger of capture by what is sometimes unkindly described as the 'gates and fences' mentality of FP.[21]

Protecting the security of equipment, personnel and facilities when they are at rest, so to speak, involves very different activities and goals than denying the enemy accurate knowledge of one's intentions and protecting plans and the same personnel and equipment when they are in motion, as it were, on operations against the enemy. FP is more concerned with robust security measures, detecting primarily human threat vectors and then conducting enforcement and disruption operations to stop them, or deterring them by visibly hardening the target. OPSEC, however, is more about retaining if not surprise then at least information advantage in the battlespace. And that depends on a detailed and accurate intelligence picture of the adversary's suite of ISR capabilities in order to limit their effectiveness through denial and deception measures. Consequently, OPSEC thinking, such as that embodied in current NATO doctrine, looks towards the command staff intelligence or J2 element for that knowledge of adversary ISR, technical and human. OPSEC, essentially, requires an MDCI approach to CI.[22]

However, even the MDCI, counter-ISR lobby has problems of its own. Even while it was the dominant approach to CI in the 1990s, MDCI thinking displayed a tendency to think of counter-ISR in the first instance as a kinetic activity. Overhead reconnaissance aircraft and drones would be shot down to blind the enemy while strikes against deployed SIGINT systems would deafen them. But in many cases ISR assets, especially high-cost highly capable capital ISR assets, prefer to operate outside the reach of kinetic countermeasures. This may be because the stand-off range of their sensors is longer than the reach of the available strike options. It may because, in the case of satellites, a kinetic kill risks blow back consequences like a space junk 'cascade' and therefore strategic consequences that outweigh the tactical gains. Or – and this is especially relevant in hybrid contexts – they may operate *into* the battlespace from *outside*, deploying into friendly sovereign territory or airspace where they are protected by the niceties of international law and the risks of unwanted strategic escalation. In such cases, the only option is to have the best possible intelligence picture of those systems and their capabilities to formulate and implement non-kinetic OPSEC

measures such as concealment, camouflage and deception, and disruption through electronic warfare (EW) where possible.

Counter-intelligence versus Counter-Intelligence?

The human threat versus multidisciplinary approaches to CI, and especially the counter-ISR branch of MDCI, bring into relief yet another fundamental tension within CI. If there is one principle that all the various competing views over security version manipulation, information advantage versus law enforcement and what hostile collection activities CI is supposed to counter largely *share* it is treating CI and an *operational activity*. But insofar as CI is treated as 'intelligence' that implies not only raw intelligence collection, be it in the service of investigations or penetration, but also *finished intelligence production*. In the wake of the Second World War, John Masterman argued that one of the main objectives of the wartime 'double-cross' programme had been to 'obtain information about the personalities and methods of the German service' which he viewed as 'knowledge of the highest importance for counterespionage purposes'.[23] By much the same token, the most recent UK joint military intelligence doctrine has highlighted the importance of 'understanding ... the intelligence threat from our adversaries.'[24] That understanding is the product of CI analysis and assessment.[25]

In yet another professional and academic lacuna, while many practitioners and observers have asserted that CI analysis is very important most tend to pass over it in surprisingly little detail.[26] Less than a handful of discussions have examined CI analysis in any detail.[27] And yet not only is analysis and assessment a vital part of CI it is central to the MDCI concept. During the heyday of MDCI in the 1990s its advocates freely admitted that most deployed CI units could do very little *operationally* about hostile SIGINT, IMINT and OSINT collection activities. Counter-SIGINT tends to be an information security (INFOSEC) and communications security (COMSEC) concern, in the Anglo-American model falling under the aegis of national SIGINT agencies. Likewise, counter-IMINT and counter-OSINT measures are OPSEC tasks. And by the same token, one might argue that asking a single, central CI organization to collect information on an opponent's full assortment of ISR assets, their capabilities, deployments and activities would be like 'trying to boil the ocean'. But countermeasures against adversary technical collection require an understanding of the capabilities the adversary has or is trying to develop. In fact, monitoring adversary ISR systems is a naturally distributed function. It falls almost by definition within the routine 'positive' military intelligence activity of a command staff J2 cell collecting and assessing on an adversary order of battle in or adjacent to that command's area of operations . Therefore, while deployed CI *operations* might be largely human threat focused, CI *analysis* can and should be a multidisciplinary (CI) undertaking.[28]

CI and Hybrid War

All of these disparate difficulties and dilemmas intertwine and reinforce one another when confronted with what is often termed 'hybrid warfare' (HW) or 'full-spectrum conflict' (FSC).[29] There are many varying attempts to define what HW/FSC entail, but one can broadly characterize such strategies as being multi-level conflict and engagement that may include, for example:

1. Overt military engagement.
2. Covert or deniable sovereign paramilitary operations.

3. Overt support to paramilitary proxies.
4. Covert support to paramilitary proxies.
5. Overt information operations through propaganda, diplomatic and political engagement.
6. 'Traditional' covert information operations through agents of influence, proxies, cover and front organisations.
7. Advanced covert information operations employing various cyber instrumentalities such as on-line equivalents of (6) as well as automated means like so-called 'bot farms' and Artificial Intelligence.

Western defence and security thinks have been struggling literally for decades over how to deal with, respond to and counter HW/FSC. There has been very little consensus on this front within proposals ranging from crafting better and more integrated strategies to deploying sub-threshold irregular forces of one's own. [30]

However, if one looks at the components of HW/FSC in intelligence terms, items 2, 3, 4, 6 and 7 are *all* directly delivered by or fundamentally enabled by hostile intelligence services. They fall clearly within the core CI triad of espionage, sabotage and subversion. Indeed, two recent RUSI reports on Russian hybrid operations in the Ukraine and more globally clearly demonstrate the central role of Russia's 'special services', particularly the Federal Security Service (FSB) and GRU in the delivery of those operations.[31] Furthermore, any direct military engagement under (1) will almost always entail a substantial ISR effort conducting 'intelligence preparation of the battlespace', and intelligence assistance to proxies will very probably entail information generated by national intelligence and state-level ISR systems. And that in turn implies that any defence against HW/FSC implies multidisciplinary counterintelligence.

The inevitable conclusion is that counterintelligence is, in fact, the actual first line of defence against hybrid warfare. And herein lies one of the most important CI aspects of the Russo-Ukrainian conflict, because it began as an asymmetrical proxy-based hybrid campaign and then escalated to symmetrical open warfare.

Ukrainian Counterintelligence Before the War

To understand the CI dimensions of the Russo-Ukraine conflict clearly it is essential to appreciate the post-Soviet legacy issues that are the underlying tectonics of the lay of the geopolitical land. From a CI point of view, the principal formative geology is the status of Ukraine occupied within what John Dziak has called the 'counter-intelligence state' of the old Soviet Union and the wider Soviet Bloc. And foremost here is the fact that unlike the other central and eastern European states within the Bloc, Ukraine, Moldova and the Baltic states never had their own, formally separate intelligence services. While the East German *Ministerium Fur Statssicherheit* (Ministry for State Security (MfS)), colloquially the 'Stasi'), the Czechoslovakian *Statni Tajna, Bezpecnost* (State Security Service or STB) and Romanian *Securitate* might have been heavily influenced by the KGB they were, in the last analysis, sovereign agencies. Indeed, recent research by, for example, Daniela Richterova, has gone some distance to demonstrate just how imperfect the alignment and coordination between central and eastern European agencies and the KGB often was.[32]

By contrast, Ukraine, the Baltics and Moldova (as well as the Central Asian republics) never had even that level of autonomy but instead were covered by branches of the KGB itself.[33] As long as the USSR survived, this permitted a certain horizontal mobility between the subordinate national KGBs and the central apparatus in Moscow. Much as there were substantial populations of ethnic

Russians in those flank states as well Balts, Ukrainians and Moldovans within Russia with intermarriage common and unproblematic, so circulation within the wider KGB community meant that Ukrainians might find themselves working for the Lubyanka or Russians posted to Tallinn or Kyiv. As long as there was a common, Soviet socialist enterprise then the national porosity within what was nominally a single agency was largely unproblematic. The breakaway of the Baltic states and Ukraine's landslide vote for independence, however, meant that such transnational cross-posting necessarily created fracture lines of affiliation and loyalty.[34] Not merely might one have Russians in a Ukrainian Agency or vice versa, one might also have ethnic Ukrainians born and raised in the Soviet era who had invested their lives, careers and commitments in a Russian-led national security culture.

At the leadership levels within the Security Service of the Ukraine (*Sluzhba bezpeky Ukrainy* or SBU) before the Crimean seizure and Donbas conflict there had long been alarming signs and indications. The first head of the SBU, Yehven Marchuk was a career Soviet Ukrainian KGB officer who had risen to be deputy head of the organisation when the USSR collapsed.[35] More alarming, however, was the background of one of his successors, Ihor Kalinin, who might have been an ethnic Ukrainian but had actually been born in the Moscow region, was a Russian citizen, and his original career had been in Russia in the *Soviet Russian,* rather than Ukrainian, KGB.[36] Similar divided loyalties affected the rank and file of the SBU, and those divided loyalties would prove instrumental in the Russian prosecution of its campaigns against Ukraine in both 2014 and 2022.

Prior to 2014, the fortunes of the Ukrainian counterintelligence rested on the political complexion of the government of the day, equally shaped by post-Soviet and even deeper political legacies. Post-independence Ukrainian politics were largely shaped by a tug of war between Moscow-oriented traditionalists who largely perceived the political separation between Ukraine and Russia as an artificial division of a single people, and a more outward looking view that saw Ukraine in a wider European context.[37] Unsurprisingly, Russophile views tended to be more prevalent in the largely Russophone east and south, while nationalist and Europhile views dominated the west and north of the country.[38] Nowhere was this more apparent than in the see-sawing alignments of successive presidents prior to the Maidan Square protests. Independent Ukraine's first president, Leonid Kravchuk, may have been the erstwhile leader of the Ukrainian Communist Power but in the wake of the 1991 Ukrainian referendum on independence he became president of the new republic and pursued a consistently nationalist agenda. But he was defeated in the 1994 election and replaced by the Russophile Leonid Kuchma. After his constitutionally limited two terms in office, Kuchma nominated as his replacement Viktor Yanokovich a fellow Russophile with close links to post-Communism oligarchs whose approach has been described as 'rational pragmatism tempered by corruption and cronyism'.[39] In the 2004 election, running against nationalist Viktor Yuschenko, Yanokovich over-optimistically claimed a victory and was congratulated by Vladimir Putin only for the claim to be challenged in the supreme court and Yuschenko declared the winner in run-off election. Yanukovich then secured the role of Prime Minister after parliamentary elections in 2006, only to lose the role at the end of 2007. He then returned to the presidency amidst widespread accusations of voting fraud in 2010. The foundations were now laid for the Maidan protests, February revolution and Yanokovich's exile, the Crimea seizure, Donbas war, and eventual 2022 invasion.

During Yuschenko's term in office his SBU chief, Valentyn Navalychenko, commenced a preliminary programme of reform and democratization, but this did not survive the 2005-6 change of government.[40] Under Yanukovich it is fairly clear that the SBU returned, at least informally, to its Cold War role of regional subdivision of Russian intelligence. According to an anonymous but

apparently well-informed 2016 study of the SBU, Kalinin's directorship 'increased Russian influence in the SBU, and enhanced existing cooperation between the SBU and FSB', as a result of which 'Russian intelligence agencies met no obstacles to the infiltration of the SBU and military intelligence [*Holovne Upravlinnja Rozvidky Ministerstva Oborony Ukrajiny* or HUR].' The depth and scale appear to have been unprecedented. Reappointed as SBU chief by the incoming 'Euromaidan' administration, Navalychenko inherited a 'nearly empty SBU headquarters in Kyiv with computers and data files having been removed and taken to Russia. When Yanukovych fled to Russia in 2014 so also did Kalinin's successor as SBU head, Oleksandr Yakymenko and four of his senior officers. With them they reportedly, 'stole or destroyed data on twenty-two thousand officers and informants and anything related to cooperation between the Ukrainian and Russian intelligence services.' According to Navalychenko: 'Every hard drive and flash drive was destroyed – smashed with hammers … it was all ash and dust.' Subsequently, according to the 2016 study, 'over 200 agents [i.e. intelligence officers], including Ukraine's counterintelligence chief, were arrested, and some have been tried for high treason.'[41]

The significance of corruption in terms of CI and security should not be underestimated. In that classic framework for discussing the motivation of agents, defectors and traitors, 'MICE' – Money, Ideology, Compromise and Ego – divided loyalties and ideological legacies may account for the ideological 'I' but endemic corruption and its cynical avarice provided fertile ground for the 'M' motivation, and probably 'Compromise' as well. The pervasiveness of corruption and its implications for the former Soviet special services was publicly detected and noted in a series of unclassified intelligence appreciations published by the Canadian Security Intelligence Service even as the USSR was collapsing in the early 1990s.[42] The impact of corruption in Federal Russia's agencies has been widely noted but it clearly undermined Ukrainian agencies far more extensively.[43] As Serhii Plokhy has concluded of corruption in the SBU: 'Charged with fighting corruption, some departments of the service became involved in corruption schemes themselves, and their officers were easy targets for recruitment by their Russian counterparts.'[44]

The Multi-Disciplinary Russian Intelligence Threat

It is worth stressing that the Russian intelligence threat is a multi-layered and multi-disciplinary one. The main the CI threat from the Russian special services originally arose from the FSB, and that has been a multidisciplinary one. The most visible facet of that FSB threat has been that from the classic human vector set of HUMINT, sabotage and subversion. Indeed, the lead role of the FSB reflected the Russian perception that Ukraine is not really an independent nation. When the Confederation of Independent States (CIS) replaced the USSR, Moscow made an undertaking that CIS states would not be targeted by the Federal Russian Foreign Intelligence Service, the SVR. But in 2004 Russia used a loophole in that commitment to establish a foreign intelligence branch *within* the FSB, the now-notorious Fifth Service. Set up in 2004, the mission of the Fifth Service was to operate within what is often referred to as the Russian 'near abroad', which meant not only CIS states like Ukraine, but also perceived historical possessions such as the Baltic states.[45] Indeed, the close cooperation between Russian and CIS states that liaison provided a natural cover for, and might even have been hard to distinguish from, penetration. The Fifth Service's mission against Ukraine covered the gamut of HUMINT, clandestine subversion and sabotage planning.[46]

With the attention given to the FSB's Fifth Service since the invasion it is easy to overlook the *technical* intelligence collection threat from the FSB. Perhaps the most visible aspect of this has been cyber exploitation and cyber attack operations by the FSB and various 'persistent threat actor'

cover and front organizations.[47] But the FSB also controls the national SIGINT function. After the Cold War, the two SIGINT directorates of the KGB were hived off to become a new agency modelled broadly on the US National Security Agency (NSA) and Britain's Government Communications Headquarters (GCHQ), called the Federal Agency for Government Communications and Information (FAPSI). In 2003, however, FAPSI was abolished and its radio frequency (RF) SIGINT transferred to the FSB.[48]

The GRU also presents a multidisciplinary intelligence threat. Its most visible roles include intelligence support to command decision-making as well as human intelligence, sabotage, assassination and other forms of irregular, hybrid warfare.[49] But it is also important to keep in mind that the GRU controls the military SIGINT function including Russia's substantial land-based, maritime, airborne and space-based SIGINT systems. It also controls Russia's air-breathing and satellite imagery and geospatial intelligence capabilities.[50] The GRU, therefore, has had a key role in conducting much of the technical collection activity against Ukraine through its substantial range of ISR platforms and sensors.

There has also been a sustained and substantial subversive threat in the form of Russia's 'compatriot' policy. Delivered chiefly within the 'near abroad' by a dedicated 'compatriot' policy ministry, *Russotrudnechestvo* (Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad, and International Humanitarian Cooperation) and international network of *Russkiy Mir* ('Russian World), in many respects the 'compatriot' policy has acted as the post-Cold War substitute for the Communist narrative and the information and influence role of organizations like the COMINTERN, its successor COMINFORM and the International Department of the Communist Party of the Soviet Union (ID/CPSU). *Russotrudnechestvo*'s overt activities include supporting and mobilizing nationalist sentiment amongst Russian ethnic and linguistic communities, promoting their disengagement from the governments and wider national communities where Russian ethnics reside in places like the Baltic states, Ukraine and across the CIS, and encouraging alignment with and loyalty to Moscow. *Russotrudnechestvo* is part of a wider 'compatriot' strategy in which grey and black propaganda and disinformation activities and deniable front organizations operated by FSB and the other special services deliver its clandestine dimensions, This is a model of operation that is more than a little reminiscent of the relationship between the ID/CPSU and Service A of the KGB's First Chief Directorate during the Cold War.[51]

Crimea and the Donbas

An immediate consequence of the Yanukovich-era's subservience to Russian interests was that, according to the 2016 SBU study: 'Counterespionage activities were curtailed against Russian intelligence activities in Crimea, paving the way for the recruitment of locals and infiltration of state institutions.' This 'laid the groundwork for Russia's rapid annexation of Crimea, while infiltration of the SBU, possession of SBU intelligence files, and the installation of GRU and FSB sleepers in the Donbas would play a strategic role in the rapid takeover of power in the Donbas by separatists in the spring of 2014'.[52] Under Yanukovych, the Russian intelligence services were kith and kin and not perceived as an intelligence requirement and target by his Russophile SBU leadership. As a result, even after Yanukovych and his allies fled to Russia and Petro Poroshenko's 'Euromaidan' administration took hold of the levers of power, it was too late for Ukrainian intelligence to rapidly alter its priorities and operational commitments and wheel east. Consequently, the SBU 'proved unable to provide intelligence to Ukrainian leaders […] about Russian plans to invade and annex Crimea or Russian training of separatists who would assist Russian "green men" (GRU special forces

without country insignia on their uniforms) in the take-over of Donetsk towns in the spring of 2014'. Instead, 'Russian intelligence officers operated throughout eastern and southern Ukraine, training and paying vigilantes to attack Euromaidan supporters and capture state buildings.'[53]

It was during the Crimea and Donbas phase that we already begin to see the counter-ISR challenge of a hybrid campaign beginning to take shape. Having already laid down the clandestine operational support infrastructure for a sustained proxy/partisan irregular warfare campaign, as well as what has become known as 'implausibly deniable'[54] combatants, Russia began to provide the kind of defence systems only nation state militaries can afford to support the partisan effort. This included not only highly capable weapons systems such as the BUK anti-air missiles that downed Malaysian Airlines flight MH 17, but also Russian Army mobile SIGINT units. These included *Svet-Ku* and *Dzudoist* vehicle-mounted SIGINT systems operating in concert with mobile jamming/interference units, coupled to Leer-3 command, control and communications (C3) vehicles to disseminate their data. By 2017 there were believed to be '19 Russian EW formations' in Donetsk and Luhansk controlled directly from Moscow by the GRU rather than under local partisan control, as well as a strategic jammer redeployed from Murmansk to Crimea.[55]

The Ukrainians, by contrast, were equipped only with aging Cold War systems and, as the conflict progressed, a fairly minimal assortment counter-fire targeting radars. Ukraine was also ill-equipped to intercept or disrupt the communications and radars used by Russian forces in the region. As one review of the situation at the time observed, this combination of SIGINT and jamming elements meant that 'Russian EW systems are able to collect information about Ukrainian positions and methods of control and can evaluate the effectiveness of short-term blocking of communications.' The result was effective Russian EW dominance in the region, with the deployed EW units being used to target and suppress not just local radio communications but 'radars, GPS and SATCOM [satellite communications] signals including Iridium and Inmarsat.'[56] During the Donbas phase, the counter-ISR competition was entirely one-sided in Russia's favour.

The 'Special Military Operation'

The opening phases of Russia's 2022 invasion were characterized by a succession of counter-HUMINT horrors that were all too much like a replay of the 2014 collapse of the SBU, as well as wholesale infiltration both of the agency and on the ground that again laid critical groundwork for the planned offensive. Serhii Plokhy has provided a concise summary of the key CI events that is worth reproducing at length. As the invasion surged past Ukrainian defences, the SBU;

> soon arrested one of their own, the commander of the Kherson anti-terrorist center, Lieutenant Colonel Ihor Sadokin, on charges of high treason. He had apparently supplied the Russians with maps of minefields and then coordinated Russian air attacks once the SBU team under his command abandoned Kherson. Zelensky demoted Sadokhin's superior, General Serhii Kryvoruchko, the head of the Kherson branch of the SBU, stripping him of his rank. Kryvoruchko and his men had apparently left Kherson on the first day of the war. It appeared that the SBU was sharing secrets with the enemy … The problems were not limited to Kherson. A few hours before the Russian invasion, General Andrii Naumov, the deputy head of the SBU in charge of internal security, fled the country. He would be arrested a few months later by Serbian authorities on charges of money laundering. The customs officers found €600,000 (about $125,000) and an undisclosed number of diamonds in his car. In July Zelensky fired [SBU chief Ivan] Bakanov, citing numerous cases of high treason by SBU

officers. A few days earlier, there had been media reports about the arrest of Oleh Kulinich, the former head of the SBU department in charge of Crimean intelligence networks. He was charged with high treason.[57]

Kulinich, it transpired, also was part of a larger network of Russophile Ukrainians in a range of highly sensitive positions centred on Ukrainian parliamentarian Andriy Derkach, a graduate of the FSB (then the Federal Counterintelligence Service or FSK) and son of a former KGB officer.[58] Kulich had also served as a significant agent of influence, facilitating *inter alia* Naumov's appointment in charge of the SBU's Main Directorate of Security.[59] Having had to essentially build an entirely new agency after 2014, Ukraine now had to undertake an intensive programme of insider threat investigations within its agencies even as those agencies were in the midst of fighting a war. And these were merely part of a much broader campaign of CI investigation of Ukraine's political and security elites.[60]

If there was any actual benefit to the Ukrainian intelligence community from the Soviet, Chekist legacy it was that they would have had an intimate knowledge of the equally Chekist 'play book' of Putin's agencies. While there has been little evidence (to date) that this had effectively hardened the Ukrainian agencies against what Julie Anderson has called 'Putin's HUMINT offensive'[61] and the 'compatriot' counteroffensive, there were strong indications they had been better prepared in terms of counter*sabotage*.

There is a tendency in many discussions of Soviet and Federal Russian special services to focus primarily on their regime-protection role, but no less central to their role at least as far back as Felikzs Dzerzhinsky and the VCheka has been the 'executive action' role of sabotage, assassination and other forms paramilitary irregular warfare. A significant part of this during the Cold War was the establishment of 'sleeper' paramilitary cells that were organized and equipped during peacetime. The intent was for these to lie fallow until the outbreak of hostilities, at which point they would be activated and mount sabotage operations against military facilities and communications and logistical infrastructure, and conduct targeted anti-neck/anti-head assassination of key figures in the adversary's politico-military leadership. Defectors such as Oleg Lyalin, who detailed KGB paramilitary war planning in the early 1970s, and Vladimir Rezun who provided similar information about equivalent GRU activities delivered by *Spetznats* special forces under GRU control, provided an alarming picture of what had previously been a rather weakly understood sabotage threat. This threat was subsequently incorporated more systematically into NATO plans and exercises.[62]

Ukrainian awareness of the threat from paramilitary 'sleeper cells' became especially acute during the opening stages of the war. In November 2021 the Ukrainian government announced that it had discovered FSB efforts to organize a coup led by an FSB officer supported by 'three defectors of Ukraine's Interior Ministry who are based in Crimea'.[63] On 13 February 2022, the UK and allies also warned that the FSB's Fifth Service was preparing additional paramilitary actions and local seizures of power.[64] On 25 February Kyiv Mayor Vitali Klitschko declared a series of curfews between the hours of 17:00 and 08:00 in response to an expected mobilization of FSB and GRU sabotage cells in support of the main Russian offensive. The curfews were heralded with the menacing warning: 'Warning! All civilians on the street during the curfew will be considered members of the enemy's sabotage and reconnaissance groups.'[65] And to a degree the feared irregular warfare offensive appeared in fits and starts, mainly in the form of GRU-controlled *Spetsnaz* saboteurs, and were largely effectively dealt with by Kyiv's defenders.[66]

Russia's HUMINT also experienced major setbacks. Russia's global efforts were decimated shortly after the invasion as a succession of countries around the world expelled identified and suspected

Russian intelligence officers from SVR, GRU and even FSB *rezidentura* operating under Embassy cover. Some 600 Russian intelligence personnel had been expelled since, with roughly 400 expelled within the first two months.[67] At the same time, the FSB's Fifth Service largely failed to deliver either accurate intelligence or an effective programme of sabotage and subversion. In part the misleading intelligence has been attributed to a reliance on information from Russophile emigres like Yanukovich and his coterie, as well as the chronic tendency of authoritarian agencies to fail to speak truth to power.[68] The failure of the Fifth Service's sabotage and subversion has typically been attributed to the endemic corruption that has afflicted the Russian special services since the end of the Cold War, noted above. The prevailing view is that the substantial funds directed to this work were mainly embezzled by self-serving Chekist officials who, like most of the rest of the world, appear not to have expected a hot war with Ukraine to ever actually happen.[69]

On the MDCI front, Russia stepped up its ISR during the run-up to the 2022 invasion. This began with Sukhoi (SU) 24 FENCER fast jets carrying Cold War-vintage ELINT pods, 'whose purpose was to map the locations of Ukrainian long-range early warning radars and radar-guided ground-based air defence systems.' At this point the FENCERs were protected from any kinetic countermeasures less by distance than by the niceties of international law. They flew their radars intelligence (RADINT) missions 'along the border of Russian and Belarus airspace', that is, within Russian airspace, at a point where open hostilities had not yet commenced between Russia and Ukraine.[70] They were not, therefore, susceptible to kinetic counter-ISR measures.

It is a standard item in discussions of CI that CI knowledge often provides what is sometimes called 'positive' intelligence, that is, intelligence about adversary capabilities and intentions rather than their narrow intelligence and espionage activities. This is especially true of counter-ISR because information on adversary ISR activities as they undertake intelligence preparation of the battlespace often features as a significant indicator in warning intelligence (see Gustafson *et al* in this issue for a detailed discussion of indicators and warning prior to the 2022 invasion). In 2022 existing air surveillance would have detected the FENCERS, but few if any significant OPSEC measures were taken and, as Gustafson *et al* note, the Ukrainian leadership appears to have been taken by at least tactical surprise, perhaps because of cognitive dissonance or sheer disbelief, and possibly also warning fatigue after months of reiterated warning of the imminence of a Russian invasion from come of their allies.

With the commencement of the invasion, Russian ISR activity escalated in quality as well as quantity. The first increment was the deployment of SU-34 FULLBACK fighter-bombers equipped with the latest UKR-RT ELINT pod capable of 'pinpointing radar positions and recording their emissions' and sending that data through a high bandwidth data link to ground stations up to an estimated distance upwards of 200 nautical miles.[71] This was then supplemented with longer endurance SIGINT platforms in the form of Ilyshin IL20M COOT-A, the Beriev A-50U MAINSTAY airborne early warning and control (AEW&C) and, most recently, the Tupolev TU-214R. The COOT-As are an aging fleet of Cold War vintage aircraft with airframes dating in some cases back to the 1960s in a fashion reminiscent of the venerable (but now decommissioned) British Nimrod. Originally primarily SIGINT aircraft, recent upgrades added side-looking phased-array radar and an electro-optical (EO) and infrared (IR) imaging suite in a nose turret. Of significantly more recent (but still Cold War) vintage, MAINSTAYs contribute to operational and tactical intelligence by providing air situational awareness and targeting support to strike operations as well a reportedly being 'outfitted with undisclosed ELINT/SIGINT equipment added … in the early 2010s'. The TU-214s are Russia's newest and most expensive air-breathing assets, indeed so expensive and so troubled in development that only two

have been delivered since 2012. The TU-214R carries comprehensive sensor suite including side-looking SAR and a wide range of SIGINT capabilities but also EO/IR systems.[72]

Technical ISR is not simply confined to the stereotypical role of target acquisition and development and battle damage assessment. ISR is also essential to the more comprehensive intelligence understanding of adversary forces. Kevin Riehle has illustrated this lucidly, noting of the rare but highly capable TU-214R that it, 'can build an electronic order of battle' of an adversary's 'electronic emitters'.[73] This is, of course, an essential input to a more comprehensive order of battle (ORBAT) for enemy forces when combined with information the rest of the human and technical ISR armature. And ORBAT analysis is an essential part of assessing that enemy's capabilities and intentions, and for any net assessment of enemy and friendly forces.[74]

The wider intelligence exploitation of ISR systems provides added significance to the destruction of two Russian A50U MAINSTAYs operating over the Sea of Azov. The first of these was the 15 January 2024 shootdown of a MAINSTAY and damage to an IL20M COOT-B airborne command post, with a second MAINSTAY downed on 23 February. As the daily UK Defence Intelligence (DI) *Intelligence Update* noted two days later after the first A50U was destroyed: 'The A-50 is critical to the Russian air surveillance picture of the battlespace'.[75] The COOT-B acted primarily as a communications platform relaying the high-bandwidth data stream from e.g. A-50U MAINSTAY to less capable command, control and communications (C3) elements on the ground capable stations. Once direct fighting broke out between Russia and Ukraine, high-flying ISR platforms were no longer protected by remaining in Russian air space, and once it entered the western reaches of the Sea of Azov the Beriev could not benefit from the stand-off range of its sensors and placed itself within the reach of the as-yet unidentified anti-air system that shot it down. Nonetheless, drawing the A50 into range and attacking it without drawing Russian counterfire against the missile batteries involved will have involved a strong ELINT understanding of Russia's ELINT capabilities combined with artful emissions control (EMCON) by the Ukrainian targeting radars.[76] Of the second downing, DI assessed that 'Russia has highly likely grounded the [A50] fleet' in the Ukraine theatre 'whilst internal investigations take place surrounding the failure to protect another high value enabler'. The consequences of the MAINSTAY losses 'significantly degrades the situational awareness provided to ground crews … a capability gap Russia can ill afford.'[77] What matters most in this incident is not that the downing of the two MAINSTAYS entailed the loss of big, expensive, high-prestige pieces of kit. What really matters is that these were kinetic counter-ISR actions and therefore, in MDCI terms, counter*intelligence* successes of some significance.

Conclusion

This discussion of counterintelligence in a still-running conflict must, necessarily, be treated as a tentative, preliminary narrative. It is also important to note that this discussion has focused entirely on the SBU. Ukrainian military intelligence, the HUR, and the foreign intelligence service that was hived off from the SBU IN 2004[78] have yet to receive the same level of attention. However, while the fine detail of the intelligence war in the Ukraine still needs to come to light it is possible to draw rather less tentative conclusions with comparatively robust levels of confidence.

One inescapable conclusion is that the Russo-Ukraine conflict has been a counterintelligence perfect storm. The country was not only confronted with an aggressive, multi-agency, multi-disciplinary intelligence threat but one that defied easy politico-military responses because of its extended

hybrid phase. Worse still, Ukraine was a nation beset by divided identities and loyalties that had roots that ran almost a century deep.

But Ukraine is not the only European state facing this kind of threat and CI challenge. Other states in the traditional Russian 'near abroad' are also regarded as renegade provinces of the Russian empire in the Putinesque worldview. Although they are NATO members, the Baltic states are both geographically exposed and potentially isolated and susceptible to similar hybrid and 'implausibly deniable' disruption. Significantly, their security services have been making intensive efforts to raise the alarm regarding escalating Russian espionage and subversion activities in the region, not merely by publishing their annual reports detailing the threat *but publishing them in English*.[79] But to one degree or another, the Russian hybrid threat from its 'special services' is one that affects all of NATO, and it is a model being followed by other adversarial states elsewhere across the globe. Jack Watling and his coauthors have argued trenchantly that 'Countering disinformation … is far less consequential that degrading the support apparatus in degrading this process' and 'undermining the human intelligence activity that supports unconventional warfare methods is vital to degrading Russia's capacity' to conduct such operations.[80] In other words, *counterintelligence* is the first line of defence not just against hybrid warfare but in the wider emerging 21st Century strategic environment.

But the riposte against hostile *technical* intelligence collection needs to be equally robust, and thoroughly integrated with 'traditional' CI against human threat vectors. And herein lies that larger CI lesson from the Russo-Ukraine conflict: counterintelligence needs to be a holistic enterprise that approaches hostile intelligence activity in the round, across all of its different threat vectors, human and technical. While the need for this is most apparent in hybrid warfare, it is not particular to it. The essence of multidisciplinary CI is a friendly interagency all-source intelligence effort *against* a hostile interagency all-source intelligence effort. Detecting, penetrating and countering the grey zone/sub-threshold leading edge of a full-spectrum offensive depends fundamentally on the most comprehensive CI understanding of the adversary's working methods, policies, practices and apparatus. But this can only be achieved when CI analysis and assessment are as developed CI operations and investigations. Nearly a generation ago, the wider intelligence community had to learn hard lessons about effectively balancing need to know and need to share. CI has yet to achieve the same balance. The warning from Ukraine is that, in many respects, Wester counterintelligence has yet to fully enter the 21st Century.

Bibliography

Anderson, Julie. 'The HUMINT Offensive from Putin's Chekist State' *International Journal of Intelligence and CounterIntelligence*, Vol.20 No.2 (2007) pp.258-316, DOI: 10.1080/08850600601079958

Axe, David. '"Blinded" Every A-50 Radar Plane The Ukrainians Shoot Down Opens A Gap In Russian Radar Coverage—A Gap The Ukrainians Can Exploit' *Forbes* 24 February 2024. https://www.forbes.com/sites/davidaxe/2024/02/24/blinded-every-a-50-radar-plane-the-ukrainians-shoot-down-opens-a-gap-in-russian-radar-coverage-a-gap-the-ukrainians-can-exploit/?sh=744fbcb717ee.

Axe, David. 'Ukrainian Crews Set A Complex Missile Trap For Russia's Best Radar Plane' *Forbes* 16 January 2024.

BBC 'Ukraine invasion: Kyiv imposes curfew amid sabotage fears' *BBC News* 26 February 2022 https://www.bbc.co.uk/news/world-europe-60539122

Clark, David D and Susan Landau 'Untangling Attribution' *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010) pp.25-40.

Cormac, Rory and Richard J. Aldrich 'Grey is the New Black: Covert Action and Implausible Deniability' *International Affairs*, Vol.94 No.3 (May 2018) pp.477–494, https://doi.org/10.1093/ia/iiy067

Davies, Philip H.J. 'ISR versus ISTAR: A Conceptual Crisis in British Military Intelligence' International Journal of Intelligence and Counterintelligence Vol.35 No.1 (2022) pp.73-100. DOI: 10.1080/08850607.2020.1866334.

Davies, Philip H. J. 'The Trouble with TESSOC: The Coming Crisis in UK and Allied Counterintelligence Doctrine' *Defence Studies* forthcoming. DOI:10.1080/14702436.2024.2303084

Development, Concepts and Doctrine Centre (DCDC). *Intelligence, Counterintelligence and Security Support to Joint Operations* (Shrivenham, UK: DCDC, 2023).

DCDC. *The Future Character of Conflict* (Shrivenham: DCDC, 2010).

DCDC. *JDP 2-00 Understanding and Intelligence Support to Joint Operations* (Shrivenham: DCDC, 2011).

Defence Intelligence. *Intelligence Update* 17 January 2024 https://twitter.com/DefenceHQ/status/1747544627257745426

Defence Intelligence. *Intelligence Update* 27 February 2024 https://twitter.com/DefenceHQ/status/1762419530356146576

Defence Intelligence. *Intelligence Update* 2 March 2024 https://twitter.com/DefenceHQ/status/1763866642541351405

Dossier Centre, *The Lubyanka Federation: How the FSB determines the politics and economics of Russia* (Washington DC: The Atlantic Council, 2020).

Dylan, Huw, David Gioe and Elena Grossfeld 'The Autocrat's Intelligence Paradox: Vladimir Putin's (Mis)management of Russian Strategic Assessment in the Ukraine War' *British Journal of Politics and International Relations* Vol.25 No.3 (2023) pp.385-404 doi.org/10.1177/13691481221146113

Fish, Tim. 'Russia Steps Up Electronic War in Ukraine' *Digital Battlespace* Vol.9 No.4 (July/August 2017) p.7.

Gabidullina, Roksana and Pierre Morcos 'Curtailing Russia: Diplomatic Expulsions and the War in Ukraine' *Center for Strategic and International Studies* 19 May 2022 https://www.csis.org/analysis/curtailing-russia-diplomatic-expulsions-and-war-ukraine.

Galeotti, Mark. 'Controlling Chaos: How Russia manages its political war in Europe' *European Council on Foreign Relations* 1 September 2017 https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/

Gentry , John A. 'Toward a Theory of Non-State Actors' *Intelligence, Intelligence and National Security* Vol.31 No.4 (2016) pp.465-489, DOI: 10.1080/02684527.2015.1062320

Giles, Kier. *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power* (London: Royal Institute for International Affairs, 2016).

Godson, Roy. *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (New Brunswick NJ: Transaction Publishers 2001).

Godson, Roy. 'General Discussion'. *Intelligence Requirements for the 1980s: Counterintelligence*. (Washington DC: National Strategy Information Centre, 1980) pp.156-158

Graham, Adrian. *Communications, Radar and Electronic Warfare* (Chichester, UK: John Wiley & Sons, 2011)

Haslam, Jonathan. *Near and Distant Neighbours* (Oxford: Oxford University Press, 2015).

Henderson, David H. *Field Intelligence: Its Principles and Practice*. (Melbourne: J. Kemp Government Printer, 1904).

Henderson, Robert D'Arcy. *Commentary: Future of ex-Eastern Bloc Intelligence Personnel* No.4 (July 1990) (Ottawa: Canadian Security Intelligence Service (CSIS), 1990).

Hyde, Lily. 'Saboteurs Spark Suspicion and Solidarity in Kyiv' *Politico* 26 February 2022 https://www.politico.eu/article/russian-saboteurs-spark-suspicion-solidarity-in-ukraine-kyiv/ [

Intelligence and Security Committee (ISC). *Russia* HC632 (London: HMSO 2020).

Interfax-Ukraine, 'State overthrow being prepared by FSB officer, three defectors from Interior Ministry – media' *Interfax-Ukraine* 27 November 2021 https://en.interfax.com.ua/news/general/782479.html

Jensen, Carl J., David H. McElreath and Melissa Graves *Introduction to Intelligence Studies* 3rd Edition, 2023).

Johnson, David E. *Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza* (Santa Monica: RAND Corporation, 2010).

Johnson, Loch K. *National Security Intelligence* 2nd Edition (Cambridge: Polity Press, 2017).

Johnson, Robert 'Hybrid War and its Countermeasures: A Critique of the Literature' *Small Wars and Insurgencies* Vol.29 No.1 (2018) pp.141-163 DOI: 10.1080/09592318.2018.1404770

Joint Doctrine and Concepts Centre (JDCC) *Joint Warfare Publication 2-00: Joint Operational Intelligence* 1st Edition. (Shrivenham, UK: JDCC, 1999).

Kalaris, George and Leonard McCoy 'Counterintelligence' in Roy Godson ed. *Intelligence Requirements for the 199s: Collection, Analysis, Counterintelligence and Covert Action* (Massachusetts: Lexington Heath 1989) pp.127-136.

Latvian Security Police *Annual Report 2013* (Riga: Latvian Security Service, 2014)

Latvian Security Police *Annual Report 2017* (Riga: Latvian Security Service, 2018)

Lutsevych. Orisia. *Agents of the Russian World Proxy Groups in the Contested Neighbourhood* (London: Royal Institute of International Affairs, 2016).

Lutsevych. Orisi ,The Long Arm of Russian "Soft" Power' *Atlantic Council: UkraineAlert* 4 May 2016 https://www.atlanticcouncil.org/blogs/ukrainealert/the-long-arm-of-russian-soft-power/

Masterman, J.C. *The Double-Cross System in the War of 1939 to 1945* (New Haven: Yale University Press, 1972).

Maximenkov, Leonid and C. Namiesniowski *Commentary: Organized Crime in Post-Communist Russia – A Criminal Revolution?* No.48 September 1994 (Ottawa: CSIS, 1994)

Meister, Stefan. *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign*. (Washington DC: Transatlantic Academy, 2016)

Miler, Newton S. 'Counterintelligence' in Roy Godson ed. *Intelligence Requirements for the 1980s Number One: Elements of Intelligence* (Washington DC: National Strategy Information Center, 1979) pp.47-60.

Mladenov, Alexander. 'Russia's Spies in the Sky' *Airforces Monthly* 241 (February 2024) pp.35-39.

N.A. 'Ukraine: KGB to Security Service of Ukraine' in Bob de Graaff and James M. Nyce, with Chelsea Locke, ed. *The Handbook of European Intelligence Cultures* (Plynouth, UK: Rowman & Littlefield, 2016).

NATO Standards Organization (NSO) *AJP 3.14 Allied Joint Doctrine for Force Protection* NATO UNCLASSIFIED (Brussels: NSO, 2015).

NSO *AJP 3.14 Allied Joint Doctrine for Intelligence, Counterintelligence and Security* NATO UNCLASSIFIED (Brussels: NSO, 2016).

NSO *AJP 3.10.2 Allied Joint Doctrine for Operations Security and Deception* NATO UNCLASSIFIED (Brussels: NSO, 2020).

Plokhy, Serhii. *The Russo-Ukrainian War* (London: Penguin Random House UK, 2023).

Polese, Abel, Rob Kevlihan and Donnacha Ó Beacháin *Small Wars and Insurgencies* special issue *Hybrid Warfare in Post-Soviet Spaces* Vol.27 No.3 (2016).

Prunckun, Hank. *Counterintelligence Theory and Practice* 2nd Edition (New York: Rowman and Littlefield, 2019).

Rayner, Gordon. 'Ukraine invasion: Kyiv imposes curfew amid sabotage fears' *The Telegraph* 25 February 2022 https://www.telegraph.co.uk/world-news/2022/02/25/gun-battle-kyiv-ambush-russian-plot/

Reynolds, Nick and

Richterova, Daniela 'The anxious host: Czechoslovakia and Carlos the Jackal 1978–1986' *The International History Review* Vol.40 No.1, (2018) pp.108-132, DOI: 10.1080/07075332.2017.1309560

Riehle, Kevin P. 'Assessing Foreign Intelligence Threats' *American Intelligence Journal* Vol.31 No.1 (2013) pp.96-101.

Riehle, Kevin P. 'A Counterintelligence Analysis Typology' *American Intelligence Journal* (AIJ) 32:1 (2015) PP.55-60.

Riehle, Kevin P. *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present* (Bethesda, MD: National Intelligence Press, 2022).

Sabbagh, Dan. 'Russia's FSB agency tasked with engineering coups in Ukrainian cities, UK believes' *The Guardian* 13 February 2022 https://www.theguardian.com/world/2022/feb/13/russias-fsb-agency-engineering-coups-ukrainian-cities

Sawka, Richard. *Frontline Ukraine: Crisis in the Borderlands* (London: I.B. Tauris, 2015).

Schultz, Richard H. & Roy Godson *Dezinformatsia: The Strategy of Soviet Disinformation* (New York: Berkley Books. 1986)

Shulsky, Abram N. and Gary J. Schmitt *Silent Warfare: Understanding the World of Intelligence* 3rd Edition (Washinton DC: Brassey's Inc. 2002).

Soldatov, Andrei and Irina Borogin 'Putin Places Spies Under House Arrest' *Centre for European Policy Analysis* 11 March 2022 https://cepa.org/article/putin-places-spies-under-house-arrest/

Soldatov, Andrei and Irina Borogin 'The Shadow War: Putin Strips Spies of Ukraine Role' *Centre for European Policy Analysis* 11 March 2022 https://cepa.org/article/the-shadow-war-putin-strips-spies-of-ukraine-role/

Soldatov, Andrei and Irina Borogin. *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: PublicAffairs, 2010)

Suvorov, Viktor. *Soviet Military Intelligence* (London: Hamish Hamilton, 1984)

Suvorov, Viktor *Spetsnaz: The Story of the Soviet SAS* (London: Grafton Books, 1987).

United State Army. *Army Regulation 381-20 Military Intelligence The Counterintelligence Program*. (Washington DC: Headquarters, Department of the Army 1993)

United States Marine Corps *MCWP 2-14 Counterintelligence* (Washington DC: Department of the Navy, Headquarters United States Marine Corps, 2000)

Watling, Jack. 'The Kaleidoscopic Campaigning of Russia's Special Services' *RUSI Commentary* 20 September 2022, https://www.rusi.org/explore-our-research/publications/commentary/kaleidoscopic-campaigning-russias-special-services.

Watling, Jack, Oleksander V Danylyuk and Nick Reynolds *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023* (London: RUSI, 2023).

Watling, Jack, Oleksander V Danylyuk and Nick Reynolds *The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022-24* (London: RUSI, 2024).

Zuehlke, Arthur A. 'What is Counterintelligence?' in Roy Godson ed. *Intelligence Requirements for the 1980s Number Three: Counterintelligence* (Washington DC: National Strategy Information Center, 1980) pp.13-39.

[1] War Office *Manual of Military Intelligence 1946 Pamphlet No.3 Counter-Intelligence – Military Security* WO279/372 The National Archive (TNA) 1.
[2] Roy Godson ed. *Intelligence Requirements for the 1980s: Elements of Intelligence* REFERENCE
[3] See, e.g. Johnson *National Security Intelligence* 116-154; Jensen *et al Introduction to Intelligence Studies* esp.211-213 and Johnson *Thwarting Enemies at Home and Abroad, passim*.
[4] For a detailed analysis of this issue, see Davies 'The Trouble with TESSOC' *passim*. At various points, this article will draw on material abstracted from that in-depth discussion.
[5] John A. Gentry (2016) 'Toward a Theory of Non-State Actors'
[6] Davies 'British Democracy in a New Age of Subversion' 5. This is also the inadequately discussed background to the ISC's complaint that the UK's Security and Intelligence Agencies (SIA) 'they not view themselves as holding primary responsibility for the active defence of the UK's democratic processes from hostile foreign interference'. See the ISC *Russia* report 10.
[7] NATO Standards Organization (NSO) *Allied Joint Doctrine for Intelligence, Counterintelligence and Security* 7-1 – 7-2, 8-1.
[8] This is most often associated with the CI provision of Ronald Reagan's Executive Order (EO) 123323 of 1981 Section 3.4, but also featured in its predecessor EO 12036 in 1978, Section 4-202 and appears in an official lexicon issued by an Intelligence Community Staff 'Intelligence Definitions Working Group' issued in 1977 CIA-RDP91M00696R000300020005-7, CIA Research Tool (CREST).
[9] War Office *Manual of Military Intelligence Pamphlet No.1 Intelligence Staff Duties* 51, WO 279/374, TNA.
[10] See, e.g. Godson 'Discussion' 156 Miler 'Counterintelligence' 49.
[11] Joint Development and Doctrine Centre (JDCC) *Joint Warfare Publication 2-00: Joint Operational Intelligence* 1A-5.
[12] NSO *Allied Joint Doctrine for Force Protection* A-14; NSO *Allied Joint Doctrine for Intelligence, Counterintelligence and Security* 8-1.
[13] This, and much of the following doctrinal discussion, is abstracted from Davies 'The Trouble with TESSOC'.
[14] Discussed at some length in Johnson *Thwarting Enemies at Home and Abroad* pp.13-19.
[15] Zuehlke 'What is Counterintelligence' 16-17.
[16] Henderson *Field Intelligence* 46
[17] There is a slight potential confusion in discussing CI as 'multidisciplinary'. The conduct of CI operations has long been multidisciplinary in the sense that both human and technical collection methods may be deployed *against* the enemy intelligence organization per the CI SIGINT and cyber examples discussed above. In this case, Zuehlke is referring to countering the *adversary's* use of technical as well as human collection.
[18] See, variously, Kalaris and McCoy 'Counterintelligence' 129-130 (who, significantly, are pitching the notion as early as 1989), United States Army *Field Manual 34-60 Counterintelligence passim*, United States Marine Corps (USMC) *MCWP 2-14 Counterintelligence* C-1 – C-23 and, from the 'counterespionage is counter-HUMINT' camp Shulsky and Schmitt *Silent Warfare* pp.114-116.
[19] JDCC *Joint Warfare Publication 2-00: Joint Operational Intelligence* 1A-5
[20] See Davies 'ISR Versus ISTAR' 78-80
[21] One can see that tug of war at work over the last decade and a half between, for example, the third edition of the UK joint intelligence doctrine and the FP influenced 2016 NATO intelligence doctrine on the one hand, and what might be called a more maneouvreist CI approach in the latest, fourth edition of the UK intelligence

doctrine. For the FP dominated approach see Development, Doctrine and Concepts Centre (DCDC) *Understanding and Intelligence Support to Operations* 2-15 – 2-16, NSO *Allied Joint Doctrine for Intelligence, Counterintelligence and Security* 7-1 – 8-8, NSO *Allied Joint Doctrine for Force Protection* 4-3, 4-11 n.37, A-13 – A-14. On the manoeuvreist approach, see DCDC *Intelligence, Counterintelligence and Security Support to Joint Operations* 85-92.

[22] NSO *Allied Joint Doctrine for Operations Security and Deception* 3 - 4, 11.

[23] Masterman *The Double Cross System* 8.

[24] DCDC *Intelligence, Counterintelligence and Security Support to Joint Operations* 88.

[25] DCDC *Intelligence, Counterintelligence and Security Support to Joint Operations* 90-91; Godson *Dirty Tricks or Trump Cards?* 187-188.

[26] Both Godson and Prunckun have nominally substantial sections on 'analysis' but in both cases these are largely concerned with the analytic aspects of CI operational activity and 'positive' intelligence exploitation of CI information but with only a handful of paragraphs on CI analysis as CI knowledge; Prunckun *Counterintelligence Theory and Practice* 23; Godson *Dirty Tricks or Trump Cards* 191-192.

[27] Confined by the length of an article, Zuehlke offers one of the most detailed discussions of CI analysis and CI knowledge pp.33-35, Kevin Riehle has, however, offered the most thorough discussion of counterintelligence analysis as a class of finished intelligence in his 'A Counterintelligence Analysis Typology' and 'Assessing Foreign Intelligence Threats'.

[28] United States Army *Field Manual 34-60 Counterintelligence* 1-7

[29] In this discussion, HW/FSC used *only* to refer to conflicts that combine symmetrical and asymmetrical engagement with state support of any non-state asymmetrical belligerents. For a range of characterizations of HW/FSC see, e.g. Johnson 'Hybrid Warfare and Its Countermeasures'

[30] For a concise and lucid overview, see e.g. Johnson 'Hybrid Warfare and Its Countermeasures'; DCDC *Future Character of Conflict* (2010 edition) 13 and *passim*; Johnson *Military Capabilities for Hybrid War*; with specific reference to the Ukraine conflict, Giles Russia's 'New' Tools for Confronting the West and the essays compiled by Polese *et al* in their special issue of *Small Wars and Insurgency.*
for Hybrid War.

[31] Watling *et al Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukraine War* and *The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022-24*, both *passim*.

[32] See, e.g. Richterova 'The Anxious Host'.

[33] With regards to Ukraine specifically, see N.A. 'Ukraine: KGB to Security Service of Ukraine (SBU) 406-407

[34] On Ukraine's referendum on secession, see e.g. Plokhy *The Russo-Ukrainian War* 2-4, 26-28.

[35] N.A. 'Ukraine: KGB to Security Service of Ukraine (SBU) p.406. There is some apparent confusion in this account about Marchuk role as 'first' SBU head because a table of SBU chairmen on p.412 gives Mykola Holushko holding the role in 1991 prior to Marchuk taking office that same year. It may that Holushko held a 'caretaker' role during the transition from Soviet Ukrainian KGB to SBU.

[36] N.A. 'From KGB to Security Service of Ukraine (SBU)' p.413.

[37] Richard Sawka has argued that the west-facing Ukrainian nationalists can be divided into two camps of their own, those who view Ukraine as a distinct ethnic and linguistic as well as geographical entity whom he refers to as 'monists', and those who view Ukraine as a civil society that is a confederal amalgam of diverse ethnic and language groups. Such an internal division has, of course, paled somewhat in significance in the face of Russian aggression. See Sawka *Frontline Ukraine*, *passim.*

[38] Plokhii *The Russo-Ukraine War* 42-48.

[39] Sawka *Frontline Ukraine* 51.

[40] N.A. . 'Ukraine: KGB to Security Service of Ukraine (SBU)' 409.

[41] N.A. . 'Ukraine: KGB to Security Service of Ukraine (SBU)' 413-414.

[42] See, e.g. Henderson *Future of Eastern Bloc Intelligence Personnel*, Maxmenkov and Namiesnowski *Organized Crime in Post-Communist Russia*

[43] N.A. 'Ukraine: KGB to Security Service of Ukraine (SBU)' 408

[44] Plokhy *The Russo-Ukranian War* 207

[45] See, variously, Dylan *et al* 'The Autocrat's Intelligence Paradox' 388, Watling 'The Kaleidoscopic Campaigning of Russia's Special Services'; The Dossier Center *Lubyanka Federation* 16.

[46] See, variously, Reynolds and Watling 'Ukraine Through Russia's Eyes',

[47] The cyber community often draws a distinction between cyber activities for espionage, referred to as cyber *exploitation* and those amounting to sabotage termed cyber *attack*. See, e.g. Clark and Landau *Untangling Attribution*.
[48] Soldatov and Borogin *The New Nobility* 249, Riehle *Russian Intelligence* p.238, 242-2. The rise and fall of FAPSI remains probably one of the most important and yet largely unexamined stories of post-Soviet Russian intelligence. The cyber side of FAPSI's role was largely transferred to the FSO.
[49] For a somewhat histrionic and dated version of the GRU's role, see Viktor Suvorov (Vladimir Rezun) *Soviet Military Intelligence passim*, more recently and sedately Riehle *Russian Intelligence passim* and Watling 'The Kaleidoscopic Campaigning of Russia's Special Services'.
[50] See, e.g., Riehle *Russian Intelligence* 239, 247-256
[51] On *Russotrudnechestvo* and the wider *Russkiy Mir* network of front and cover organizations see, variously, Lutsevych *Agents of the Russian World* and 'The Long Arm of Russian "Soft" Power', Meister *Isolation and Propaganda* and Galeotti 'Controlling Chaos'. For detailed accounts of 'compatriot' policy operations in the Baltic states an especially detailed discussion in Latvian Security Police *Annual Report 2013* 7-12 and *Annual Report 2017* 7-19; on the Service A-ID/CPSU dynamic, see Schultz and Godson *Dezinformatsia passim*.
[52] N.A. . 'Ukraine: KGB to Security Service of Ukraine (SBU)' 413.
[53] N.A. . 'Ukraine: KGB to Security Service of Ukraine (SBU)'415.
[54] Haslam *Near and Distant Neighbours* 278-279; Cormac and Aldrich 'Grey is the New Black' *passim*.
[55] Fish 'Russia Steps Up Electronic War in Ukraine'
[56] Fish 'Russia Steps Up Electronic War in Ukraine'
[57] Plokhy *The Russo-Ukranian War* 206-207.
[58] Watling *et al*. *Preliminary Lessons from Russia's Unconventional Operations* 6-8.
[59] Watling *et al*. *Preliminary Lessons from Russia's Unconventional Operations* 8-9.
[60] For an overview of Russian penetration of Ukraine, see Watling *et al*. *Preliminary Lessons from Russia's Unconventional Operations* 4-19.
[61] Anderson 'The HUMINT Offensive from Putin's Chekist State'
[62] Gordon Brook-Shephard *The Storm Birds* 198, 225-6. Brook-Shepherd specifically references NATO's 1985 BRAVE DEFENDER exercise, although he acknowledges that Rezun's reporting was probably only one of a number of factors in BRAVE DEFENDER's intensified force protection focus. Rezun subsequently became a popular author of somewhat overwrought but influential accounts of the GRU and *Spetznats*, writing under the name Viktor Suvorov.
[63] Interfax-Ukraine, 'State overthrow being prepared by FSB officer, three defectors from Interior Ministry – media'
[64] Sabbagh 'Russia's FSB agency tasked with engineering coups in Ukrainian cities, UK believes'
[65] See, e.g. Lily Hyde 'Saboteurs Spark Suspicion and Solidarity in Kyiv'.
[66] Plokhy *The Russo-Ukrainian War* 165.
[67] See e.g. Gabidolina and Morcos 'Curtailing Russia: Diplomatic Expulsions and the War in Ukraine'; see also Watling *et al The Threat from Russia's Unconventional Warfare Beyond Ukraine* 8.
[68] Dylan *et al* 'The Autocrat's Intelligence Paradox' *passim*; Plokhy *The Russo-Ukrainian War* 163, 166.
[69] There still appears to be considerable uncertainty about what did or did not transpire vis vis the underperformance of the Fifth Service in the opening phases of the war, with some confusion about the status of Fifth Service head Sergei Baseda, and for the balance of power/responsibility between the FSB and the GRU. See, variously, Dylan *et al* 'The Autocrat's Intelligence Paradox' 390; Soldatov and Borogin 'Putin Places Spies Under House Arrest', 'The Shadow War'; Plokhy 166.
[70] Alexander Mladenov 'Russia's Spies in the Sky' 33-34.
[71] Mladenov 'Russia's Spies in the Sky' 34, 35.
[72] See variously, Mladenov Russia's Spies in the Sky' 35,37 and Riehle *Russian Intelligence* 249-251.
[73] Riehle *Russian Intelligence* 250.
[74] For a more general description of the SIGINT contribution to ORBAT analysis Graham *Communications, Radar and Electronic Warfare* 4-14.
[75] Defence Intelligence *Intelligence Update* 17 January 2024 and 27 February 2024.
[76] Axe 'Ukrainian Crews Set A Complex Missile Trap For Russia's Best Radar Plane'
[77] Defence Intelligence *Intelligence Update* 2 March 2024; see also Axe '"Blinded"'.
[78] N.A. . 'Ukraine: KGB to Security Service of Ukraine (SBU)' 407.

[79] For the annual reports of the three Baltic security services, see: Latvia: https://vdd.gov.lv/en/useful/annual-reports; Lithuania https://www.vsd.lt/en/activities/activity-reports/; Estonia: https://kapo.ee/en/content/annual-reviews/.
[80] Watling *et al The Threat from Russia's Unconventional Warfare Beyond Ukraine* 13, 33.