Counterintelligence: Enduring Lessons from the Cold War

https://www.e-ir.info/2017/09/18/counterintelligence-enduring-lessons-from-the-cold-war/

DANIELE HADI IRANDOOST, SEP 18 2017

The inquiries that went into the conduct of counterintelligence before the events of 9/11 all concluded that the intelligence community was unprepared against contemporary challenges to national security from non-state terrorist groups, in a rapidly globalised and technologically advanced world.[1] Indeed, it was assumed that many lessons learnt from the previous era, which was characterised by an ideological struggle between two superpowers, were all irrelevant now. As will be demonstrated in this essay, however, this view does not hold ground upon closer examination. Specifically, the essay will examine counterintelligence lessons drawn from case studies in the Cold War and compare their applicability to contemporary counterintelligence affairs

But before going any further, it is first crucial to define counterintelligence. Broadly speaking, counterintelligence concerns activities undertaken by intelligence agencies to protect the society, particularly from espionage, covert action and deception that may be undertaken by a range of actors including states, terrorist groups, malicious individuals, organisations and criminals amongst others.[2] Overall, these are done either proactively or defensively: whilst the former refers to activities that attempt to 'manipulate' an enemy, the latter is about actions that stop the enemy in its tracks. Examples of the former may include, for instance, planting double agents or spreading propaganda on media, whilst 'defensive' examples might consist of identifying weaknesses within security programmes, or even of gathering intelligence (of any type) to find and apprehend, say, traitors within one's own intelligence system.

With those in mind, the primary objective of this essay is to identify and examine *enduring* lessons from various case studies in the Cold War for counterintelligence operations today. Overall, four lessons will be examined: 1) understanding the context, 2) mitigating the politicisation of intelligence, 3) adapting 'structures', and 4) recognising the everlasting relevance of the inevitability of 'counterintelligence failures'. Due to the breadth of each lesson, the essay will focus only on two specific case studies (one from the Cold War and one from the post-Cold War period) for every lesson, as sample studies for understanding the broader lessons. Overall, these case studies were chosen mainly because of their relevance as well as significance to their related lessons. It is worth noting the contemporary case studies are drawn from within the US only, though the lessons may as well apply to other intelligence communities around the globe.

To begin with, the first lesson concerns the significance of understanding contexts within which counterintelligence activities operate. The term context is used here to refer to such things as social and cultural trends (differing worldviews or narratives, in a sense) locally and globally, strengths and weaknesses as well as *modus operandi* of an enemy (and certainly one's own), not to mention past experiences and history, amongst others. The purpose, then, is to understand how the bigger picture will shape enemy intelligence operations – objectives and conduct – and to adapt counterintelligence accordingly.

As an illustration, a relevant case study includes the influence of changing social and historical trends on the motivations behind espionage in the Cold War. According to Stan Tayler and Daniel Snow, spies are motivated for various reasons including money, ideology, ingratiation, disgruntlement, fantasy, self-importance/ego, and kinship – though almost in all cases these are combined with one another to varying degrees.[3] The authors also note that the

two most dominant motivations during the Cold War were money and ideology, at least in the case of those 139 Americans (from 1940 to 1994) who were officially charged as traitors.[4] But the more interesting point is how these trends, in terms of their dominance, changed from one time/space (context) to another. The obvious evidence here, of course, is how ideology became less significant from the early 1960s onwards, unlike money which became the most dominant of all (perhaps denoting the declining popularity of communism as a result of public knowledge of Stalin's purges, not to mention the rising popularity of consumerism and wealth amongst the peoples in the West).[5] A good representation, in this instance, of the broader picture is of course the comparison between the Cambridge Five, the likes of the Rosenbergs or Klaus Fuchs, who were ideologically motivated in the main, and Robert Hansen and Aldrich Ames who began their espionage largely because of financial reasons later in the Cold War.[6]

Applied to the present, the most relevant case study is indeed the shifting of motivations towards religious values advocated primarily by Islamic terrorist groups seeking information on, say, US intelligence capabilities or advanced nuclear technology. As Harber pointed out, terrorist groups nowadays do not have the same amount of resources that states (such as the Soviet Union) had in recruiting agents during the Cold War, leaving them instead the option of exploiting religious values or a sense of kinship, only.[7] The overall lesson here, therefore, is the necessity to understand the context in order to gain insight into, for instance, the ways in which an enemy may operate under certain circumstances and to use this knowledge to adapt counterintelligence operations (defensive and/or proactive), leading not only to effective prioritisation, but ultimately to successful counterintelligence.

Having said that, understanding the context is not sufficient on its own, for to have an accurate picture of the context one is also required to have balanced frameworks of analysis. Probably, the most prominent obstacle against this type of balance concerns the politicisation of intelligence, reinforced by such cognitive biases as underestimation/overestimation, mirror-imaging, or confirmation bias, amongst others. The lesson here, in this sense, is to recognise politicisation as a limitation and to try to actively minimise its influence when undertaking counterintelligence operations.

To demonstrate how and why this is important, the Soviet politicisation of intelligence around the Able Archer exercise offers an appropriate case study. Able Archer refers to a NATO annual exercise in 1983. What was particularly significant about the event was that even though there were no plans by the West to attack the Soviet Union, the Soviet leadership along with a number of high-level officials (for instance, the head of the KGB, Yuri Andropov) had become fearful of an illusory attack from the West, disguised by the annual exercise.[8] Developed over a long-term period prior to the actual event (as a result of different historical trends and events, such as Reagan's announcement of the Star Wars programme and the Soviet Union's overall perception of inferiority in economic and military terms compared to the West), the Soviet fear and pressure from the top was to such an extent that the spies on the field were not only *disc*ouraged from offering their own more accurate views, but were instead encouraged to look for the wrong information (such as, counting the number of lights switched on at night in governmental departments) to confirm false assumptions held by the leadership in Moscow.[9] Indeed, anyone who did otherwise was expected to suffer some sort of punishment from their superiors. But what is vital against this background was the possible danger of a nuclear war from a mere politicisation of intelligence which could have led to irreversibly grave consequences.[10] Had the Soviet leadership recognised previous cases of politicisation, and had they combined this awareness with an understanding of the historical context to adapt their counterintelligence operations (Operation Ryan, for one) the likelihood of this dangerous scenario could have been alleviated.

With those in mind, one may find comparable case studies in the US today: the most prominent being the 2003 Iraq War.[11] As is most commonly known, the intelligence that was used to support the invasion of Iraq was largely politicised to confirm the inaccurate beliefs of the political leadership.[12] And as has similarly been witnessed by many throughout the world, the consequences of doing so have not been so pleasant either. The leadership believed that Saddam was housing and developing WMDs in secret and in violation of international treaties and sanctions. In fact, the belief was so ingrained in the minds of the likes of Bush that they only selected those bits of intelligence that confirmed their biases – not unlike the Soviet leadership during the Able Archer crisis. Hence, the enduring lesson here is to recognise the existence of the politicisation of intelligence in their different forms and to actively strive to minimise their harmful consequences (say, through context-driven structural adaptations) having in mind at the same time the cognitive biases that could reinforce their development.

In turn, that leads to our third lesson: that to remove structural obstacles to effective counterintelligence is a necessity. The third lesson, in this sense, requires the responsible actors to adapt structures around counterintelligence operations – of course, having in mind the other two lessons examined earlier – so as to maximise even further the efficiency and success of such operations. Indeed, it is important to note that structure refers here to a broad number of elements that affect the conduct of counterintelligence operations. Some of the more significant ones include organisational structures within the intelligence community (such as, the extent to which intelligence should be shared and coordinated with other intelligence branches without compromising security), extent of regulation over liaison with foreign intelligence agencies, legal and oversight frameworks, security programmes (vetting, background checks, extent of classification and so forth), not to mention bureaucratic processes involved within the intelligence cycle (appropriate dissemination methods, for one).

A successful Cold War case study that illustrates this issue in practice is the ratification of the Foreign Intelligence Surveillance Act (FISA) in 1978 which, in short, allowed intelligence agencies to prosecute traitors more easily than was previously possible. Before FISA, evidence that was collected secretly could not be used in public courts not only for fear of compromising valuable sources and methods of espionage, but also because of the American courts' rejection of illegally obtained evidence. The ratification of the Act, however, made it not only possible for evidence to be used in court, it also made sure that sources and methods remained secret: all because evidence was now accepted in a secret court.[13] As Tayler and Snow observed, the result was intriguing: following the ratification, the number of those prosecuted for reasons of espionage increased exponentially, compared to the previous period (23 per cent caught and prosecuted from 1945 until 1977, compared to 38 per cent from 1978 until 1994).[14] What is noteworthy in this example, therefore, is how structural obstacles were removed according to the context of US domestic law, leading as a result to more effective counterespionage operations.

A contemporary case study that follows along the same lines, but perhaps slightly excessively is the enactment of the Patriot Act in October 2001, as a result of the 9/11 terrorist attacks. On the one hand, it may be pointed out that the Patriot Act was crucial for removing obstacles to more widespread surveillance powers and capabilities which intelligence agencies so often desire. The argument goes, of course, that more surveillance always results in better and more effective counterintelligence operations (including against terrorism).[15] On the other hand, it may be noted the Act has been criticised for the intrusive powers it has provided for the intelligence agencies.[16] Having in mind that this could potentially undermine human rights (taking into account the slippery-slope argument) and therefore public support for the agencies, and that since public support is an important factor behind the functioning of intelligence agencies,[17] it may be maintained that the structural changes have gone too far, and so need to be reversed or even altered. The overall idea, then, is to maximise success as far as is possible through structural changes, whilst considering also different contexts as well as dangers that could arise from the politicisation of intelligence – that is, the previous two lessons.

Lastly, the fourth lesson concerns the 'inevitability of counterintelligence failures' even if the above lessons are exercised with utmost effort.[18] Broadly speaking, this argument refers to intrinsic limitations found within the human mind, namely that cognitive biases can never go away and that it is never possible for a human mind to have a *complete* picture of the world, implying that structural as well as operational weaknesses are always bound to be found, or even *not* found considering the fact that there will always be 'unknown unknowns' and that these may not be so easily avoidable.[19] The many counterintelligence failures in the Cold War are indeed a clear manifestation of this phenomenon. It is difficult to say whether the failures recounted above could have been avoided – with certainty – had the people responsible tried their best to fulfil the lessons learnt earlier.

One example that particularly illustrates how this may be the case is the debate on whether Oleg Penkovksy was a Soviet double agent, tasked to deceive the Americans as part of a larger deception operation, planned by Khrushchev, to force Kennedy to remove missiles from Turkey, in exchange for removing Soviet missiles in Cuba.[20] Although this argument is highly controversial it underscores the lesson noted above: that despite all the ways in which counterintelligence analysts might have attempted to validate Penkovsky's role as a double agent, one was still not entirely sure at the time, or even now in some ways, of the whole picture – particularly when having in mind the so-called 'wilderness of mirrors' which so often accompanies counterintelligence operations. What this example demonstrates of course is that problems arise not just when there are 'unknown unknowns', but also when

even there are 'known unknowns'.

A case study that reflects a similar pattern in recent years in the US most noticeably includes the 'tactical' unawareness of intelligence and policing agencies before 9/11 of the exact location and timing of the attacks, despite a more general 'strategic' knowledge of an impending attack on the US.[21] All of which indicate – perhaps surprisingly – an irony inseparable from intelligence activities: that despite their responsibility to predict the future and protect their society, intelligence agencies are merely made up of fallible humans who are not – as it were – omniscient beings. Overall, the lesson is to recognise that mistakes are inevitable and are even a natural part of human life and that nothing can in fact be realistically done to change the course of events at all times and at all places.

On the whole, this essay proposed four lessons for the conduct of successful counterintelligence operations in the contemporary US, drawn from various case studies in the Cold War: sequentially, these included understanding the context, minimising the politicisation of intelligence, adaptation of structures, as well as awareness of the inevitability of 'counterintelligence failures'. To a large extent these lessons were chosen not only because of their flexibility but also because their breadth allowed for addressing the root causes of counterintelligence failures directly. As one characterised by secret 'wars in the shadows', the Cold War appeared the most suitable period for an inquiry of this sort compared to any other in history. And although previously there have been attempts within the literature to learn from past failures, rarely have they brought together 'tactical/operational' lessons into one overarching 'strategic' lesson as was done in the essay: this especially applies to the first and third lessons. In any event, what is above all important to remember is that not only is there a need for moderation in all things, but that continuities do indeed occur in history; that even though platforms change from one place and time to another, lessons learnt in one period may well be applicable to another and therefore relevant depending on the specific context. The applicability of counterintelligence lessons drawn from the Cold War for contemporary US challenges more than attest to this point.

Bibliography

9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.: U.S. Government Printing Office, 2017.

Andrew, C. M., and O. Gordievsky. *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985*. London: Sceptre, Hodder & Stoughton, 1993.

Aldrich, R. "Dangerous Liaisons: Post September 11 Intelligence Alliances". *Harvard International Review* 24, no. 3 (2002): 49-54.

Betts, R. K. "Analysis, War, and Decision: Why Intelligence Failures are Inevitable". *World Politics* 31, no. 1 (1978): 61-89.

Epstein, E. J. *Deception: The Invisible War Between the KGB and the CIA*. New York: Simon and Schuster, 1989.

Haddick, R. "Strategic Error: When the Big Picture Misses the Point". *Foreign Policy*, 2012. Accessed April 1, 2017. http://foreignpolicy.com/2012/08/24/strategic-error/.

Harber, J. R. "Unconventional Spies: The Counterintelligence Threat from Non-State Actors".*International Journal of Intelligence and CounterIntelligence* 22, no. 2 (2009): 221-236.

Kahn, D. "An Historical Theory of Intelligence". *Intelligence and National Security* 16, no. 3 (2001): 79-92.

Lowenthal, M. M. *Intelligence: From Secrets to Policy*. 6th ed. Los Angeles; London; New Delhi: CQ Press, 2015.

Omand, D. "Can We Have the Pleasure of the Grin Without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light?". *Intelligence and National Security* 23, no. 5 (2008): 593-607.

Pillar, P. R. “Intelligence, Policy, and the War in Iraq”. *Foreign Affairs* 85, no. 2 (2006): 15-27.

Schaefer, B. “Forecasting Nuclear War: Stasi/KGB Intelligence Cooperation under Project RYAN”. *Wilson Center*. Last modified 2014. Accessed April 1, 2017. https://www.wilsoncenter.org/publication/forecasting-nuclear-war.

Scott, L. “Intelligence and the Risk of Nuclear War: Able Archer-83 Revisited”. *Intelligence and National Security* 26, no. 6 (2011): 759-777.

Shulsky, A. N., and G. J. Schmitt. *Silent Warfare: Understanding the World of Intelligence*. 3rd ed. Washington, D.C.: Brassey’s, 2002.

Taylor, S. A., and K. Buchanan. “Treason: ” ‘Tis Worse Than Murder” “. In *The Oxford Handbook of National Security Intelligence*, ed. by K. J. Loch, 518-536. Oxford; New York: Oxford University Press, 2010.

Taylor, S. A., and D. Snow. “Cold War Spies: Why They Spied and How They Got Caught” *Intelligence and National Security* 12, no. 2 (1997): 101-125.

U.S. Department of Defense. *DoD News Briefing – Secretary Rumsfeld and Gen. Myers*, 2002. Accessed April 1, 2017. http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

Notes

[1] For example, see 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: U.S. Government Printing Office, 2017), pp. 103f.

[2] A. N. Shulsky and G. J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Washington, D.C.: Brassey’s, 2002), p. 99.; M. M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington, D.C.: CQ Press, 2003), pp. 113.

[3] S. A. Taylor and D. Snow, “Cold War Spies: Why They Spied and How They Got Caught”,*Intelligence and National Security* 12, no. 2 (1997), pp. 102ff.

[4] Ibid. p. 103.

[5] Ibid. p. 105.

[6] Ibid.; S. A. Taylor and K. Buchanan, “Treason: ” ‘Tis Worse Than Murder””, in*The Oxford Handbook of National Security Intelligence*, ed. K. J. Loch (Oxford; New York: Oxford University Press, 2010), pp. 528f.

[7] J. R. Harber, “Unconventional Spies: The Counterintelligence Threat from Non-State Actors”, *International Journal of Intelligence and CounterIntelligence* 22, no. 2 (2009), p. 223.

[8] C. M. Andrew and O. Gordievsky, *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985*, (London: Sceptre, Hodder & Stoughton, 1993), pp. 31ff.

[9] B. Schaefer, “Forecasting Nuclear War: Stasi/KGB Intelligence Cooperation under Project RYAN”, *Wilson Center*, last modified 2014, accessed April 1, 2017,

https://www.wilsoncenter.org/publication/forecasting-nuclear-war.

[10] L. Scott, “Intelligence and the Risk of Nuclear War: Able Archer-83 Revisited”, *Intelligence and National Security* 26, no. 6 (2011), pp. 759-777.

[11] It is worth noting, the case studies examined in this section are considered to be counterintelligence examples because, broadly speaking, they were primarily concerned with the protection of their respective societies, which meant also that intelligence was perceived as a tool for defence than offence, on the main. It may be useful here to consider David Kahn's understanding of intelligence as well (slightly out of context, however): that intelligence is essential for defence but only an accompanying characteristic of the offence, possibly proposing that counterintelligence on the whole should be our main starting point when attempting to examine intelligence activities. D. Kahn, "An Historical Theory of Intelligence", *Intelligence and National Security* 16, no. 3 (2001), pp. 85f.

[12] P. R. Pillar, "Intelligence, Policy, and the War in Iraq", *Foreign Affairs* 85, no. 2 (2006), pp. 21ff.

[13] Taylor and Snow, "Cold War Spies", pp. 110ff.

[14] Ibid., p. 113.

[15] M. T. McCarthy, "Recent Development", *Harvard Journal on Legislation* 39, no. 2 (2017), p. 435.

[16] Ibid.

[17] D. Omand, "Can We Have the Pleasure of the Grin Without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light?", *Intelligence and National Security* 23, no. 5 (2008), p. 606.

[18] This is a slight variation of Richard Betts' argument that 'intelligence failures are inevitable'. R. K. Betts, "Analysis, War, And Decision: Why Intelligence Failures Are Inevitable", *World Politics* 31, no. 1 (1978), pp. 61-89.

[19] U.S. Department of Defense, *DoD News Briefing – Secretary Rumsfeld and Gen. Myers* , 2002, accessed April 1, 2017, http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

[20] E. J. Epstein, *Deception: The Invisible War Between the KGB and the CIA,* (New York: Simon and Schuster, 1989), p. 80.

[21] R. Haddick, "Strategic Error: When the Big Picture Misses the Point", *Foreign Policy*, 2012, accessed April 1, 2017, http://foreignpolicy.com/2012/08/24/strategic-error/.

Written by: Daniele Hadi Irandoost
Written at: Aberystwyth University
Written for: Dr Warren Dockter
Date written: April 2017