February 2023

Australian National University
National Security College

A Guide to Subversive Statecraft

A Submission to the Select Committee on Foreign Interference through Social Media

By Dr. William A. Stoltz, Senior Fellow at the National Security College, the Australian National University

About this Submission

This submission is made on behalf of **Dr. William A. Stoltz,** Senior Fellow at the National Security College at the Australian National University (ANU). In 2022 he published a major piece exploring the future of Australia's approach to covert action, *A Regrettable Necessity: The Future of Australian Covert Action.*

While the views expressed in this submission are not representative of any institutional position on behalf of the ANU, this submission is informed a research project undertaken in collaboration between the National Security College and the Centre for the Study of Subversion, Unconventional Interventions and Terrorism at the University of Nottingham.

The following researchers are acknowledged as playing a pivotal role in the research behind this submission:

Prof Rory Cormac is a fellow of the royal historical society and professor of international relations at the University of Nottingham. His research specialises in intelligence, covert operations, and subversion. He has written six books, most recently *How To Stage A Coup and 10 Other Lessons from the World of Secret statecraft (Atlantic, 2022)*.

Prof Andrew Mumford is a professor of war studies at the University of Nottingham. His expertise lies in the political management of warfare on which he has published widely. His books include *Proxy Warfare* (Polity, 2013) and *The West's War Against Islamic State* (IB Tauris, 2021)

Katherine Bayford is a doctoral researcher at the University of Nottingham and a research fellow at SUIT. Her PhD is on the exercise of power through military and cultural means.

Dr Thomas Eason is a research fellow at SUIT. His expertise lies in foreign policy analysis, and has published on secrecy, security, and covert actions in peer reviewed academic journals, including *Intelligence and National Security* and *The British Journal of Politics and International Relations*.

David Andrews is a Senior Policy Advisor at the National Security College at the Australian National University. He has previously worked in multiple roles in the Australian Department of Defence and is completing his PhD in International Relations at La Trobe University.

Overview

Foreign interference undertaken online via social media is one facet of how states undertake what is described here as **subversive statecraft** – a spectrum of typically deniable activity intended to subvert and sabotage target states, organisations, and individuals while reducing the risk of retaliation and escalation to USING conventional force. The variation of terms and concepts for describing this activity is indicative of the challenge governments and private firms face to build a common working understanding, let alone a consensus on joint responses that improve resilience. Accordingly, this submission is offered to the Committee as a resource to place online foreign interference in the larger context of subversive statecraft operations for which it is deployed.

Key judgements

I. Subversive statecraft can be divided into information, political/economic, and paramilitary activity.
II. The nature of secrecy (exposure and acknowledgement) is crucial for cutting through jargon like hybridity, grey zones etc. and understanding how and why states seek to subvert and sabotage others.
III. Subversive statecraft is a force multiplier and is typically only a contributing factor to a wider strategic campaign. It cannot be understood in isolation from other tools of statecraft and from internal events in the target state. Instances detected occurring online via social media need to be evaluated in a wider context of activity to determined relative effectiveness.
IV. Aims are often intangible: to subvert and reduce trust in institutions rather than ambitiously to change regimes or engineer explicit policy shifts.
V. States operate on a scale of directness: mapping the relationship between state and non-state actors (whether local influencers, front organisations or rebel fighters) is essential to move beyond simplistic notions of binary state “sponsorship”.
VI. States face trade-offs when attempting to subvert others: secrecy puts a ceiling on impact and outsourcing or operating indirectly decreases control.
VII. Success is determined not only by output metrics but by outcomes (although these are difficult to measure and highly contested).
VIII. Exposure of subversion does not necessarily equate to its failure.

1. Subversive Statecraft

All states engage in diplomatic influence operations. Subversive statecraft, also known as interference or intervention, is more controversial. Subversive statecraft takes place against an international background of so-called grey zone, hybrid, or ambiguous activity. It challenges norms, blurs lines between war and peace, and is often conducted in an (im)plausibly deniable manner. The role of secrecy, exposure and acknowledgement are key to understanding the contemporary international environment and cut through the recent proliferation of buzzwords. Subversion can be exposed but not acknowledged – and still be successful. Secrecy, however, puts a ceiling on impact.

1.1 Influence versus Subversive statecraft

All states seek to influence foreign governments. Influence is a vital part of statecraft, spanning various spheres of diplomacy (public, cultural, economic, political etc.). **Diplomatic influence is different from interference or intervention**, which is often more subversive.

Subversive statecraft can take many forms, at varying degrees of deniability, risk, and violence. They can be categorised into three types (see figure 1.1 below):

- Propaganda and Information activity (see chapter 2);
- Political and economic action (see chapter 3);
- Paramilitary action (see chapter 4).

States conduct such activity both openly and covertly. Targeted killings by drone strikes are conducted both openly and covertly; propaganda is both attributable (white) and unattributable (grey/black) depending on the source; electoral interference can involve open promise or threats, or it can involve rigging the ballot.[1]

Online and cyber activity does not constitute a distinct category of subversive statecraft. Instead, it is a means or platform of delivery. Propaganda, for example, now takes place increasingly online. Cyberattacks constitute a modern form of sabotage. The internet has not revolutionised the nature of subversion. Overplaying the novelty and distinctiveness of cyber risks reinventing the wheel, overplaying the impact of its wide reach, and forgetting wider historical or conceptual lessons about what it can and cannot achieve.

Types of subversive statecraft do not exist in isolation. For example, information operations may lay the groundwork for a coup d'état or shape the narrative around a targeted killing or proxy war.

Similarly, subversive statecraft, especially when deniable, does not exist in isolation from conventional diplomatic influence. Leaders do not face a choice between covert or overt action; it is misleading to think of it as a "third option". Instead, subversive (covert) means of influence or intervention exist alongside standard diplomatic, economic, and military activity. At the extreme end, a state will not conduct an assassination or targeted killing against a target not already subject to diplomatic influence measures.

[1] Amy B. Zegart, *Spies, Lies and Algorithms: The History and Future of American Intelligence* (Princeton University Press, 2022): 175.

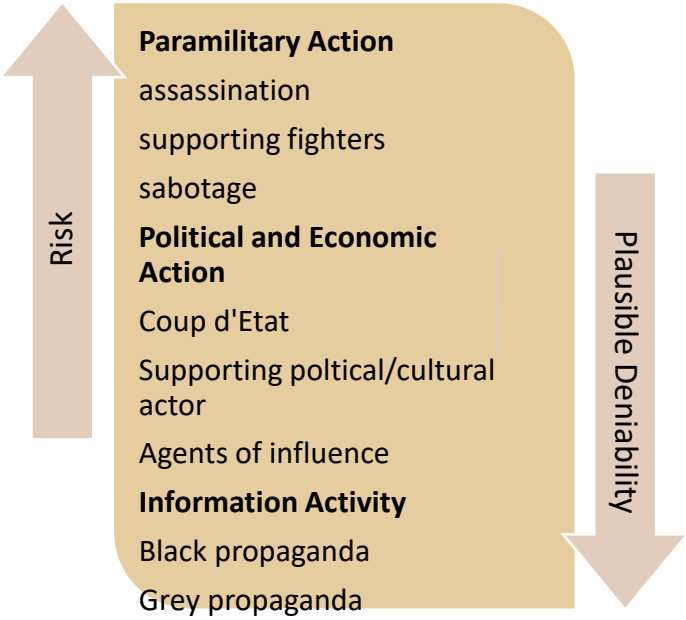

Fig 1.1 A "ladder of escalation"[2]

1.2 "Grey Zones": Secrecy, Exposure and Acknowledgement

Much subversive statecraft operates in so-called "grey zones" characterised by ambiguity and (im)plausible deniability. This is not new; states have operated in the blurred lines between war and peace for centuries. Neither is it conceptually clear: the rapidly proliferating range of buzzwords, from hybridity to non-linear warfare, is confused and references a bewildering range of military, political and economic developments.

This lack of clarity turns upon the nature of secrecy, exposure, and acknowledgement. **Many covert actions are hardly covert at all; subversive statecraft designed to be secretive is often anything but**. Policymakers and scholars mistakenly cling to the idea of plausible deniability, assuming that anything exposed is a failure. This is not the case.[3] Subversion, from influence to paramilitary operations, can be:

i) **Untraceable**. The hand of the sponsoring state is designed to be undetected by all audiences. At best there should be no suspicion.
ii) **Plausibly deniable**. The identity of the sponsor cannot be proved and, given lack of evidence to the contrary, the sponsoring state can claim that the actions others observe – and almost all covert operations are observable in some way – were sponsored by someone else.[4]
iii) **Implausibly deniable**. There may be probability and evidence of state involvement, but the state considers it politically feasible to deny complicity in public statements.

Subversive statecraft exists on a scale of exposure and ambiguity (figure 1.2 below). **Crucially, exposure does not necessarily mean failure**. States use non-acknowledged – but exposed – activity, from assassination attempts to propaganda, to send a message to adversaries.

[2] Adopted from Damien Van Puyvelde, Rory Cormac, Calder Walton, 'Qu'est-ce qu'une action clandestine réussi?' in Julian Fernandez et al (eds.) *Les Nouvelles Formes de Guerre* (Le Rubicon, 2022): 89.
[3] Rory Cormac and Richard J. Aldrich, 'Grey is the New Black: Covert Action and Implausible Deniability', *International Affairs* 94/3 (2018): 477-94.
[4] Michael Poznansky, 'Revisiting Plausible Deniability', *Journal of Strategic Studies* 45/4 (2022): 511-53.

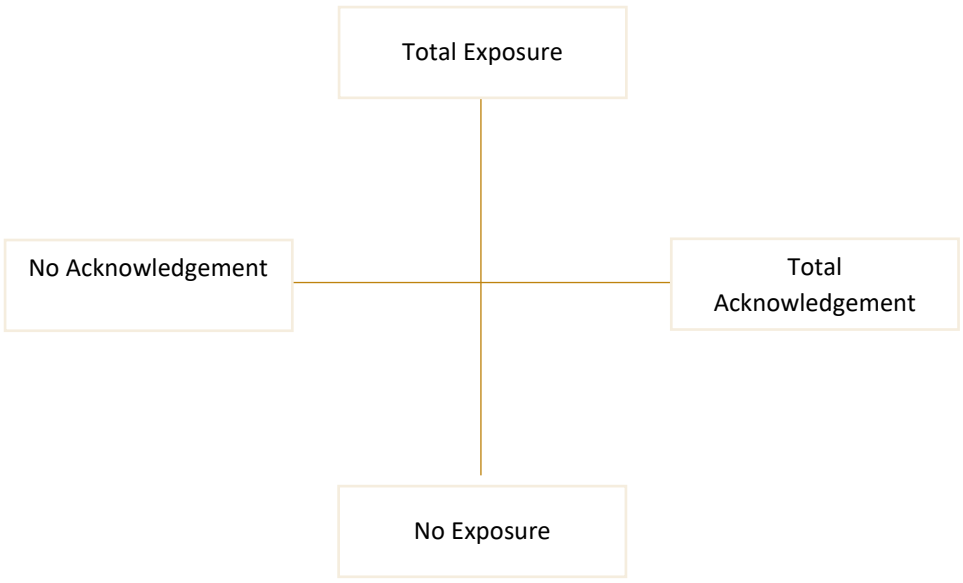

Fig 1.2: Scales of exposure and acknowledgement

States calibrate secrecy closely with their objectives: some objectives necessitate untraceable operations; other objectives, such as eroding trust or inducing paranoia, require some level of exposure or implausible deniability.

Traditional diplomatic influence activities take place in the upper right-hand quadrant: they are exposed and acknowledged. Covert subversive statecraft takes place on the left-hand side. Some activities will receive neither exposure nor acknowledgement; some will be exposed but not acknowledged (e.g. implausibly deniable proxy wars); most will fall somewhere in between. **As secrecy breaks down, exposing covert subversive statecraft will not be enough to counter it. Instead, it becomes the subject of competing cross-cutting claims and counterclaims amidst a sea of confusion rather than secrecy**.

1.3 Impact and Trade-offs

Leaders face significant constraints when deploying subversive statecraft. Operating entirely overtly can draw public criticism and create negative political consequences. Operating secretly allows deniability and reduces costs. However, **secrecy creates a ceiling limiting impact**: if a state wants to maintain an element of plausible deniability it must keep its activities at below the level where they become too obvious or provable.

States might therefore choose to outsource subversion to proxies or commercial companies, but **an indirect approach comes at the price of control** – which again might decrease impact. A range of proxies are available, from those directly paid or sponsored by the state to those acting more independently but with overlapping interests. The further away from the state, the more deniable, but the less control. Countering subversive statecraft necessitates a thorough understanding of the relationship between these actors.

States therefore face trade-offs between secrecy, scale, and control (see figure 1.3 below). The more deniable, the less impactful; the more control, the less secrecy; the more secrecy, the less control, and so on. **Subversive statecraft is about carefully calibrating secrecy and scale**.

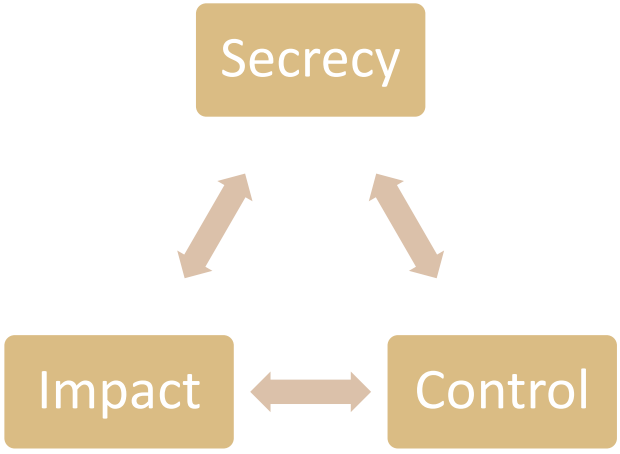

Fig. 1.3 Trade-offs

Given these limitations and trade-offs, subversive statecraft can only achieve so much. It works as a force multiplier in conjunction with other methods. Covert campaigns are best placed to achieve disruption, subversion, and confusion rather than more ambitious goals of regime change or outright victory in a civil war.

1.4 Taxonomy of Subversive statecraft

Putting all this together, subversive statecraft can be broken down into the following dimensions. Mapping an activity onto each will enable a sophisticated understanding of subversive statecraft

Objectives	**Secrecy**	**Means**	**Directness**	**Impact**
Regime change	Untraceable	Information	State actors	Outputs
Influence	Plausibly deniable	Political/Economic	Paid agents	Outcomes
Subvert/Disrupt	Implausibly deniable	Paramilitary	Witting collaborators	Beyond the immediate target (e.g. eroding trust in democracy)
Signal			“Useful idiots”	Perceptions of success

2. Propaganda and Information Operations

Influence operations seek to shape thoughts and ultimately behaviour in a manner conducive to the sponsor. Aims vary from promoting a positive image of the sponsor to disrupting targets and undermining wider trust. Influence operations are not ends in themselves but seek to facilitate a particular policy. States engage in such operations overtly (using avowed sources) and covertly (unattributable or fake sources). Intended levels of exposure – untraceable, plausibly deniable, or implausibly deniable – are carefully calibrated depending on the aim. Exposure does not necessarily mean failure. Regardless of source, influence operations draw on a range of content, from facts to outright lies, again depending on the aim. A more nuanced understanding beyond truth or lie and beyond overt or covert is essential to understand how influence operations work and how to counter them.

2.1 Introduction

All states engage in influence operations designed to shape thinking and behaviour. The vast majority of this is done openly and involves dissemination of facts (often spun or selectively edited). Many states also engage in subversive unattributable or covert influence operations. The majority do so by targeting their own populations in order to promote the image of the ruling regime. Fewer states use covert influence operations to target audiences beyond their borders: a covert means of foreign policy execution.

States known to engage in covert influence operations include China, Ecuador Egypt, France, various Gulf States, India, Iran, North Korea, Pakistan, Russia, Saudi Arabia, the UK, the US, and Venezuela.

Subversive statecraft operations can encompass a broad range of activities, from overt to covert, truth to lie (and everything in between).

2.2 Aims

Influence operations are becoming bolder and brasher, and conducted at a far higher tempo. They are more active and less measured.[5] At the same time, big data, computational propaganda and Artificial Intelligence, and the rise of the influence industry allows more micro-targeting of messages.

Despite this, the fundamental aims and principles remain stable. In some cases, as targets and larger social media organisations become more adept at responding to inauthentic networks, states (notably China) are returning to local human influencers.

2.2.1 Force multiplication

All influence operations aim to leverage traditional diplomatic or military activity. Subversive information campaigns do not exist in isolation. They are force multipliers, which lay the groundwork to make e.g. diplomatic negotiations more favourable or to pave the way for e.g. a tightening of economic sanctions. Such campaigns also multiply the effects of other types of subversive statecraft, for example softening a target in advance of political subversion (see Chapter 3). It is therefore essential to consider them in the context of the policy they are promoting rather than in isolation. Propaganda is not an end in itself; it should not be evaluated or countered as such.

2.2.2 Influence

The most obvious aim is to **influence targets' thoughts and behaviours, inducing them to act in a manner favourable to the sponsoring state**. Operations can:

i) **Discredit the target** and turn audiences against them, often by exposing misdeeds and contradictions.

[5] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, (Macmillan USA): 7.

ii) **Divide the target**, again by exposing misdeeds and contradictions, to turn audiences – such as terrorist groups or ruling parties – against each other and distract them from conducting their activity.
iii) Exaggerate levels of opposition to a regime in order to destabilise that regime or encourage those plotting against it. This is sometimes known as **coup-baiting**.

Such operations, designed to promote a coherent narrative, are becoming more difficult in today's fragmented media landscape. Co-opting or controlling few mass media channels is less influential than it once was, given the proliferation of informal channels and the blurred lines between producers and consumers.

2.2.3 Disruption and Confusion

Influence operations can aim to **chip away at the target's narrative and/or undermine trust more generally**. They flood the information sphere with multiple – often contradictory – narratives to sow confusion or discord, distract attention, and undermine authority.

States do not expect audiences to believe every message but rather seek to induce doubt into the credibility of the target, encourage audiences to question the authenticity of other information, and induce wider cynicism.

In a fragmented media landscape, negative disruption is easier than positive promotion.

States will do so because:

i) They believe in zero-sum gains: eroding trust in the target enhances the sponsor's security.
ii) They hope to exploit paralysis and distraction amongst the target to advance their own agenda unencumbered.
iii) They hope to legitimise the state's own model of governance and ease its rise.

2.3 Exposure

Depending on the aim, influence operations cover the spectrum of exposure and acknowledgement. All covert subversive operations will remain unacknowledged, but not all are designed to stay secret. They can be untraceable, plausibly deniable, and implausibly deniable. **Exposure does not necessarily equate to failure**.

Different audiences may be subject to different levels of exposure. An operation might be untraceable to the public audience but implausibly deniable to the target's counterintelligence agencies. This might be entirely deliberate depending on the aim of the operation, especially if the **state intends to communicate covertly with a rival and/or use the influence operation as leverage**. Such operations need to:

a) Have a clear signalling function or message, underpinned by credible cost of the activity
b) Calibrate exposure carefully. Some operations require complete secrecy of the sponsor in order to have maximum impact upon target audiences. Other operations require at least suspicion of the sponsor, in order to signal messages to the intended audience (which might be different from the immediate audience).

2.4 A Spectrum of Sources: from White to Black

2.4.1 White Sources

Most influence activity is overt, attributable (known as "white" material) and rarely subversive.

Channels for white material include:

- Official government statements or communications.

- Official government social media activity.
- State-funded/sponsored media, whether foreign or domestic facing.

2.4.1 Grey Sources

A sliding scale of covertness exists. White material lies at the one side. Black material (see below), with a fake source, lies at the other. In between are multiple shades of grey. **The shade denotes the extent to which the source is hidden not the accuracy of the content**.

Grey material is that which is unattributable and authorship is ambiguous. Channels exist far beyond inauthentic social media activity. They include:

- Off the record briefings – oral or written – with friendly journalists, government officials, thinktanks and/or academics.
- Laundering of white material produced in state-sponsored media through syndication agreements with independent international media, or just hoping the international press covers the story without publicising the source.
- Planting articles directly into newspapers via journalistic contacts.
- Planting articles inside genuine media agencies via agents, informal contacts, or local influencers, which will then be distributed to unwitting news outlets.
- Coordinating authentic, bottom-up, collectives of social media users (including beyond the biggest platforms and including using Artificial Intelligence).
- Working through local influencers.
- Outsourcing influence campaigns to private actors.

2.4.2 Black Sources

Black material is more controversial, traditionally more time-consuming, and is used less frequently by states. Unlike grey material, black material creates a fake source either to incriminate a target or to increase the perceived legitimacy of the message. Channels include:

- Forged material supposedly by hostile (state or non-state) actors, including state-funded news agencies or front organisations.
- Fake radio stations (or other media outlets) supposedly run by e.g. exiles, rebels etc.
- Fake organisations created to disseminate material covertly written by the state, including but not limited to thinktanks, resistance movements, civil society, media agencies, and individual social media users.
- Hacking and manipulating social media profiles, opinion polls, blogs etc.
- Astroturfing (using fake profiles and inauthentic networks to manipulate social media to create the impression of a genuine grassroots movement).

2.4.3 Use of Grey and Black Sources

First, Grey/Black sources increase the credibility of the message amongst the target audience, thus making it better placed to **influence thoughts and behaviour**.

Second, Black material can **disrupt, divide, and discredit** a target by:

- Spreading paranoia within a target group by, for example, manipulating social media profiles.

- Encumbering the adversary with costly and timely counterintelligence investigations trying to determine a) if the document is genuine and b) where it came from.
- Framing targets. Forgeries – whether analogue or digital – can be written in such a way that if/when the target state realises the material is forged, they wrongly pin the blame on a different sponsor.

Third, a flood of implausibly deniable fake sources can sow confusion, induce cynicism, and cause the audience to question the veracity of wider information. It can **undermine trust** and create exploitable paralysis.

Success therefore comes in many guises, and it is important to map the nature and purpose of the source. **Exposure could be exactly what the sponsor intends** in so far as it undermines wider trust, draws attention to a particular issue and/or makes the state appear a disproportionately powerful actor in the world of subversive statecraft.

2.5 Content: spreading truths and lies

2.5.1 Source vs Content

Subversive statecraft operations run along two axes. The source, from white to black, (section 2.4 above) constitutes one; the accuracy of the content constitutes the other. Often **commentators wrongly conflate the two, leading to a simplistic misperception of what constitutes disinformation and how states engage in subversion**.

Some influence operations are acknowledged and truthful (the top left quadrant of figure 2.1 below). This would include, for example, public health campaigns. Some can be acknowledged but deceitful (the bottom left quadrant). This is increasingly common in a "post-truth" world where populist leaders escape consequences despite openly misleading audiences. Messages can also be accurate but spread by fake sources (the top right quadrant). This approach is sometimes used by liberal democracies reluctant to lie but wanting to use fake sources to bolster credibility of the message (see, for example, British propaganda activity in the Cold War). Finally, activity can consist of lies spread through fake sources: doubly deceitful (the bottom right quadrant).

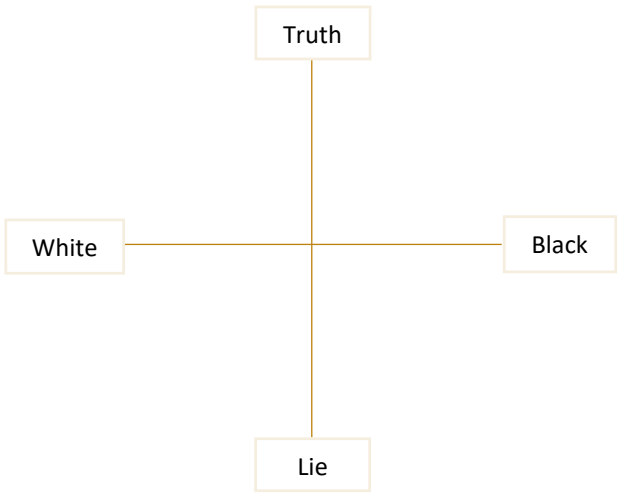

Fig.2.1 The Twin Axes of Truth

2.5.2 Disinformation vs Misinformation

Disinformation, according to popular definition, constitutes false information spread deliberately in an attempt to gain an advantage. By contrast, **misinformation**, constitutes false information shared inadvertently. It does not seek to gain advantage through deceit, and so constitutes a lesser crime.

Unfortunately, this neat distinction is not helpful in practice. First, it is difficult to judge intent. Motives may never be proved, thus making intent a poor line in the sand when differentiating between acceptable and unacceptable behaviour. Second, it is difficult to judge objectively what is true. Third, states launder untruths through people who genuinely believe them by, for example, deliberately amplifying erroneous findings made by fringe scientists, cultivating local influencers, or by stoking conspiracism by giving a platform to conspiracy theorists. Fourth, states illicitly acquire true information and use it out of context to gain an advantage (e.g. through blackmail or hack and leak operations). This is sometimes termed **malinformation**.[6]

States disseminate content across the truth/lie spectrum, depending on the objective:

Outright lies

Even outright lies tend to be believable and might have a kernel of truth in them. Depending on the objective, lies can be risky. Exposed lies decrease the credibility of an actor or influence campaign. According to NATO, 'indisputable facts' are necessary to withstand scrutiny, and false information can undermine the credibility of future operations, leading to short-term wins at the expense of longer-term problems.[7]

By contrast, exposed lies can also induce cynicism and chip away at perceptions of what is accurate and what is false. This might be the aim of the sponsor.

Emotional/religious/ideological "truths"

Some factually inaccurate content is designed to compel audiences to believe in something that feels right, regardless of evidence, by appealing to emotional truths or beliefs as a form of ideological supremacy. It puts beliefs over facts, rendering fact-checking as a means of countering influence activity difficult to achieve.[8]

Amplifying fringe actors

Rather than spreading lies directly, states bring fringe actors into the mainstream by giving them a prominent platform. Similarly, states stoke existing conspiracism by amplifying certain voices. In both cases, states cultivate witting and unwitting proliferators of its narratives. The state does not have to lie itself to spread lies but relies on networks of influence and amplification.

Hack and Leak

States might not create the material at all, but instead steal and release it *en masse* or to targeted audiences. This is not new, but, in the digital age is known as Hack and Leak and exists at a far greater scale than in the past. The most common aim is to discredit a target in order to gain an advantage.

[6] Alicia Wanless and James Pamment, 'How Do You Define a Problem Like Influence?', *Journal of Information Warfare* 18/3 (2009): 1-14.
[7] Ministry of Defence, *Allied Joint Doctrine for Psychological Operations*, Allied Joint Publication 3.10.1 (NATO Standardization Office, 2014): 1-6.
[8] Giles, Keir, *Moscow Rules: What Drives Russia to Confront the West* (Brookings Institution Press, 2018): 110.

Case study: China and the COVID pandemic, 2020

Chinese influence campaigns in response to the COVID pandemic demonstrate elements of this taxonomy. The initial aim was to distract from the emerging crisis. They did this through crude use of inauthentic social media accounts blaming Hong Kong democracy protestors for exaggerating the threat. When this failed, the aim was to multiply China's overt diplomatic response by praising China's role as a global leader in managing pandemics. Inauthentic networks promoted hashtags praising Chinese assistance to countries like Italy, whilst also spreading doctored videos to give the impression of local Italians thanking China. This complemented overt media.

As the pandemic spread, the aim became more negative: to criticise democracies' weak responses, thus legitimising China's system of government. China stoked panic and exploited existing political divisions, especially in the US. Means included inauthentic networks, text messages and text messaging apps. The aim was also to distract. Official – overt – sources complemented the covert campaign. State-owned newspapers and government spokespeople peddled conspiracies about potential US origins of the virus, amplifying any epidemiologist casting doubt the Chinese origin. Twitter removed almost 24,000 accounts deemed part of a coordinated influence campaign, as well as a further 150,000 accounts designed to amplify the content. In response, China now increasingly uses individual local human influencers.

2.6 Violence for psychological effect

The Soviet idea of disinformation – or *dezinformatsiya* – was not limited to images or written/spoken word. Instead, it expanded to 'incorrect or imaginary pictures of reality', which would take hold in the mind of the target and induce them to make decisions beneficial to the Soviets.[9]

This idea is a longstanding one. It echoes the anarchist notion of propaganda of the deed from the late nineteenth century and remains relevant today.

Sabotage, or other forms of violent activity, can have a primarily psychological purpose. This might be to:

- **Discredit** actors, through e.g. Russia desecrating Jewish graves in Ukraine and blaming the local government.
- **Divide** actors, through e.g. spraying racist graffiti in an area with a high density of immigrants.
- **Signal** displeasure, through e.g. sabotaging a gas pipeline.
- **Spread fear and justify emergency measures**, through e.g. false flag terrorist attacks.

It is crucial to differentiate between sabotage operations (see Chapter 4) and those with a predominantly psychological motive, in which violence is secondary.

2.7 Potential impact

2.7.1 Measuring success

It is difficult to quantify success, especially of loosely targeted operations seeking intangibly to reduce wider trust. How influence campaigns are publicly discussed can be as consequential as the actual influence campaign itself. In talking up the threat or over-exposing, the target can inadvertently bolster the state's work by generating a sense of the sponsor's potency, reducing trust in other sources of information, and exacerbating pre-existing divisions. Exposure can be counterproductive and must be carefully calibrated.

[9] Calder Walton, 'Inside the Disinformation Forever War', *Engelsberg Ideas*, 18/12/20.

Some influence operations depend on the target overreacting and mistaking wide reach for high impact.

2.7.2 Limitations

Unattributable, but especially fake, sources decrease state control over narrative.

First, if using a fake source, governments are compelled to adopt a particular tone and language in order to make the source credible. Forging an Islamist terrorist social media channel, for example, might not be credible without violent imagery and anti-western rhetoric. These **rhetorical devices then distort how readers interpret the ostensibly accurate message**.

Second, the globalised media environment decreases control further. A message intended for one audience might **"blowback"** (in CIA parlance) to the domestic audience of the sponsoring state. Alternatively, the propaganda might be picked up in different states around the world in a manner which might be counterproductive. States will be unwilling to acknowledge sponsorship of the narrative, allowing it to perpetuate further. Unintended consequences are more likely still if the operation is designed to sow chaos or undermine trust rather than anything more tangible / tactical.

Third, **despite dominating attention, it is not clear whether large scale social media activity causes significant impacts**. For example, there is no academic consensus that trolls and bot networks swung the 2016 US presidential elections.

Fourth, outsourcing to private companies comes at a cost. Whilst "disinformation for hire" is a booming industry allowing states to increase plausible deniability and outmanoeuvre social media companies, trade-offs exist. Private firms might overstep their briefs; they might **go for quick – and cheap – wins based on misleading metrics**; they might act on the (mis)perceived intentions of the state or generally be poorly tasked by state clients who misunderstand what can and cannot be achieved; they might compete and cut across each other thereby undermining an effective narrative. The quest for deniability comes at the cost of control.

Case study: Russia and success through overreaction

Russia has developed a reputation for engaging in high-tempo influence operations using inauthentic social media networks. Much of this is comparatively unsophisticated, but the so-called firehose of falsehoods has a wide reach. Intelligence chiefs now warn that giving too much attention or publicity to such campaigns risks turning them into successes. When the aim of Russian propaganda is to spread confusion and undermine trust in democracy, then its success counterintuitively thrives on the oxygen of publicity. Discussion of the Russian hidden hand in the US has perhaps undermined trust in US democracy as much as the operations themselves could have done. It decreases trust in what is real and what is not and provides a convenient scapegoat to mask internal divisions.

Exposure can make the adversary look more powerful than it is. Since 2014, public discussion of Russian influence operations transformed Putin into a perceived master of covert operations. Only the invasion of Ukraine dispelled this. So often influence operations work simply because audiences think they work; believing in success is to affirm success.

3. Political and Economic Activity

Subversive statecraft most often operates below the level of regime change, spanning political, cultural, academic, and commercial activity. States work through a wide range of actors, from intelligence officers to unwitting so-called "useful idiots" in order to create an environment amenable for their preferred policies to flourish. Political and economic activity exploits existing internal division, supports exiting opposition figures, and works alongside more conventional open influence work. It is intangible, subversive, pernicious, and difficult to spot. Such activity is often discreet and unacknowledged given its subversive nature, but increased secrecy leads to less impact, creating a trade-off.

3.1 Introduction

Hostile states subversively influence, interfere with, or intervene in, the political and economic conditions in a target state. The scope to do so, whether by overt or covert means, is vast: from funding political parties and meddling in elections, to shaping academic debate and constraining supply lines.

Ambitions often lie far below the goal of regime change, despite regime change dominating discussion. The extent to which states operate covertly, alongside overt methods, depends on whether they have the clout to ride out potential backlash but also on leaders' appetite for risk. Secrecy creates a ceiling for impact. **States do not choose to interfere overtly or covertly, but rather operate on a spectrum of secrecy alongside, and to multiply, more conventional open means**. It is rare and usually counterproductive for states to use standard means of diplomatic influence to achieve one objective but deploy covert political influence to achieve a competing – more subversive – objective against the same target. This makes it difficult to isolate covert political activity.

Economic interference activity is designed to cause political effect and is interwoven with political operations. Consequently, it is included within this chapter.

3.2 Aims

3.2.1 Regime Change

The most ambitious aim is regime change, whether through electoral interference or staging a coup.

Plenty of examples exist, most recently Russian attempts to interfere in the 2020 US presidential election and in the 2022 "referendum" on the Russia/Ukraine border. Historically, the US and the Soviet Union (and then Russia) have interfered in at least 117 elections worldwide since 1945.[10] The CIA also supported numerous coups in the early Cold War era, as did the UK, France, and others. Such ambitious activity takes place comparatively infrequently. **It is complicated to achieve, increasingly difficult to keep secret, and risky to undertake**.

3.2.2 Below Regime Change

States are far more likely to pursue less ambitious aims below the level of regime change. These include:

- **Influencing the legislative agenda** of a state or multilateral organisation.
- **Shaping the policy of a political party or campaign**.
- **Shaping the parameters of political debate**, by manipulating the salience and political palatability of certain ideas.
- **Finding vulnerabilities**, such as in electoral bodies or policymaking processes, which could be exploited at a later date.

[10] Dov Levin, *Meddling in the Balance Box: The Causes and Effects of Partisan Electoral Interventions* (Oxford: OUP, 2020): 52.

- **Undermining trust** in democracy broadly or in a specific election.
- **Undermine confidence in wider values**.
- **Subverting** the target by eroding the strength of the target state, usually from within. The aim is to disrupt, distract, and divide the government, destabilise it and/or keep it off balance.

Even activity which appears to be regime change often has lesser ambitions in reality. Regarding electoral interference, for example, rather than putting a new government in power, states instead aim to sow divisions and undermine trust in democracy (or in the specific election result).

The aim can be **positive**: to portray the hostile state in a positive light and promote favourable policies. It can also be **negative**: to sow confusion, breed insecurity and uncertainty, and undermine faith in institutions of authority, so as to create favourable conditions for the beneficiary. **The overarching aim is to create an environment amenable for the state's preferred policies to flourish**.

Case study: the 2016 and 2020 US presidential elections

Russia famously interfered in the 2016 US election, aiming not only to favour Donald Trump but also to provoke and amplify social discord within the United States more widely – and below the level of influencing the outcome of the election.

Multiple states covertly interfered in the 2020 election, including Russia, Iran, and Venezuela. Whilst different states supported different candidates (Russia still denigrated Biden, whilst Iran denigrated Trump), once again all states sought to exploit political divisions and subvert American democracy more broadly. Success therefore lies beyond engineering the outcome of an election.

3.3 Means

Covert political and economic influence can take myriad forms, many of which are legal and semi-overt.

3.3.1 Subversion

Subversion unfolds over three stages:

i) Penetrate key political, social, and industrial/commercial groups within the target.
ii) Exploit divisions, set groups against each other, and attack weak spots to
   a. Soften up social structures and political/commercial institutions ready for influence (or, less likely, capture).
   b. Tie down or distract social structures and political/commercial institutions to create favourable conditions and clearing the way for the hostile state
   c. Disintegrate social structures and political commercial institutions altogether
iii) States can then undermine – and potentially even detach – loyalty and weaken the target's will.[11]

3.3.2 Malign Finance of Parties, Individuals and/or Campaigns

Means include:

- Legal but hidden donations through **strawman corporate entities or shell companies**.

[11] See Paul Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations* (Quadrangle, 1954).

- **Malignant parent companies** bypass laws banning foreign companies from making political donations or loans by creating a local subsidiary through which to funnel money. This is rare.
- **NGOs can act as conduits for foreign powers to fund parties and/or influence elites**, including as a proxy for malign finance and as agent provocateurs. For example, in 2020 Russia funded a Ghanaian non-profit organisation to stoke online racial tension in the US.[12]
- **Cryptocurrency**, which is an unregulated market that can swiftly be turned into realised cash.
- **Bribery for political influence** becomes more likely in states with fewer anti-corruption laws. For example, Russian oligarch Yevgeny Prigozhin uses political-economic methods of covert influence that include bags of cash, armed forces, and online trolls in order to indebt African leaders to the Kremlin.[13]
- **Blackmail for political influence** is rare.

Case study: Chinese political interference

China's United Front Work Department uses diaspora to advance Chinese interests. In 2010, Canadian intelligence warned that several provincial cabinet ministers and government employees were agents of influence. In 2014, an Australian senator accepted money and gifts totalling around AU$1.5m from Chinese entities, some of which seemingly exploited loopholes and restrictions against foreign donations. In 2017, New Zealand intelligence investigated a Chinese-born politicians who had served on New Zealand's select committee for foreign affairs, defence, and trade. He was a United Front operative. In 2021, the UK accused a Chinese national of coordinating covertly with the United Front Work Department to interfere in British politics and disguising the origins of political donations.

3.3.3 Manipulating elections (beyond campaign finance)

- **Rigging electoral systems**, through manipulating voting mechanisms, voter registration databases etc. This is potentially impactful in terms of altering vote outcomes but is particularly difficult to achieve. Crucially, these means might aim to reduce trust or increase paranoia, rather than change regimes.
- **Intimidating voters** is an analogue means of changing votes or forcing certain voters to stay at home. Russia used intimidation during the sham referendum on Ukrainian territory (2022).
- **Information activity** (see Chapter 2).

3.3.4 Shaping Academic and Cultural Discourse

Subversive political influence extends beyond formal politics to subverting, shaping, or manipulating other groups.

Activities include:

- **Establishing student organisations** or encouraging existing organisations to mobilise against dissident views. The US State Department, for example, accused the Chinese Students and Scholars Association of both monitoring and mobilising students.[14] In Australia, 'Chinese embassy officials in Canberra gave

[12] Clarissa Ward, et al., 'Russian election meddling is back – via Ghana and Nigeria – and in your feeds,' *CNN*, 11/4/20.
[13] Ilya Rozhdestvensky, et al., 'Master and Chef: How Russia interfered in elections in twenty countries," *Proekt*, 11/4/19; "Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed," *Bellingcat*, 14/8/20.
[14] US Department of State, *The Chinese Communist Party on Campus: Opportunities and Risks* (2020).

training to hundreds of CSSA students to form 'security squads' to help drown out protesters during the visit of Premier Li Keqiang to Australia'.[15]

- Pressuring universities to suppress **critical narratives** in teaching and research, through intimidation of academics. For example, Chinse-linked actors have forged resignation emails from academics critical of China.
- **Establishing cultural education centres**. The most famous example is Confucius Institutes, partially funded by China, operating on university campuses. Critics accuse them of fostering a climate of self-censorship within western universities.
- **Cultivating sources among the diaspora** to promote particular narratives and suppress others overseas. China's United Front Work Department forms the most prominent example today. It works through the Chinese diaspora living in almost 180 countries overseas, many of whom have non-Chinese citizenship, unobtrusively providing funding to various groups deemed valuable.

3.3.5 Commercialisation of Political Influence

States can work through or target commercial entities to achieve political influence.

- Authoritarian regimes **use state-owned or backed companies to gain competitive advantage** over rivals which are not are commercially independent. For example, in Gulf states like the UAE, the security and intelligence regime extends into industrial and economic sectors.[16]
- Intelligence services can **recruit sources inside commercial entities**. This is ostensibly for espionage and surveillance purposes but has potential for influence. For example, Saudi Arabia recently recruited two sources inside Twitter to help the state monitor dissidents.[17]

3.3.6 Economic influence

Interfering in a state's economy is more difficult today than in the twentieth century, owing to increased globalisation and inter-connectedness of the world economy. Likewise, the banking system is built on confidence; exposure of attempts to manipulate bank accounts could therefore cause uncontrollable blowback. Despite this, possibilities include:

- **Spreading counterfeit money**. For example, Pakistan has frequently been accused of flooding India with counterfeit money so as to disrupt its economic stability.[18]
- **Manipulating bank accounts**.
- **Supply chain manipulation**. This is less likely on the competitive open market but there is scope in areas which are restricted or under sanctions, thereby giving external actors more scope for control. For example, supply chains to the Iranian nuclear programme are vulnerable to manipulation.
- **Promoting and sustaining industrial action**. It can be difficult to identify such activity, especially given that states facing industrial action are quick to blame hidden hands rather than examine internal conditions in their own states. The most famous example is American support for a general strike in British Guiana in the 1960s.

---

[15] Foreign Affairs Committee, *Cautious embrace: defending democracy in an age of autocracies* (UK Parliament, 2019).
[16] See Matthew Hedges, *Reinventing the Sheikhdom: Clan, Power and Patronage in Mohammed bin Zayed's UAE* (Hurst, 2021).
[17] US Department of Justice, 'Two Former Twitter Employees and a Saudi National Charged as Acting as Illegal Agents of Saudi Arabia,' Press Release 19-1206, 7/11/19.
[18] Rhys Blakely, 'Pakistan is blamed by Indian officials for flood of counterfeit cash,' *The Times*, 6/11/09.

3.3.7 Coups

States can **work with internal opposition forces to promote coups**. Coups are the 'infiltration and seizure of a small but critical segment of the state apparatus, and then using this to displace the government from its control of the remainder.'[19]

External support includes:

- Funding coup plotters.
- Propaganda to whip up popular protests.
- Encouraging coup plotters with the promise of political support and recognition.
- Intelligence support.
- Providing paramilitary forces or mercenaries.
- Giving refuge or sanctuary.

Externally supported coups may be most associated with the Cold War (notably the US in Iran and Guatemala in 1953 and 1954 respectively) and the period of decolonisation (notably the UK in the Persian Gulf and France in Africa); but they still exist today. In 2016, for example, Russia supported a failed coup attempt in Montenegro in a bold attempt to prevent the state from joining NATO.

Crucially, external forces only ever support pre-existing opposition actors inside the target state; **agency is predominantly internal**. For example, German intelligence thwarted a coup plot in 2022. Whilst reports suggested a potential Russia connection to the plotters, the internal driving force was domestic far-right nationalism and conspiracism.[20]

3.4 Mapping State "Sponsorship"

State involvement in political and economic interference exists on a spectrum. Even so, it is too often reduced to "state sponsorship" of a coup or regime change etc.

Involvement ranges from, at one end, the beneficiary state conducting the influence directly itself. This might take place, for example, through undercover intelligence officers. At the other end, states can enable an outcome perhaps by turning a blind eye to existing developments or by offering light coordination of existing actors. In between, and with varying degrees of proximity, lie outcomes which are state-linked or affiliated. See figure 3.1 below.

[19] See Edward N. Luttwak, *Coup d'Etat: A Practical Handbook*, revised edn (Harvard University Press, 2016).
[20] Brendan Cole, 'How Germany's Far-Right Coup Plot Is Linked to Russia', *Newsweek*, 12/8/22.

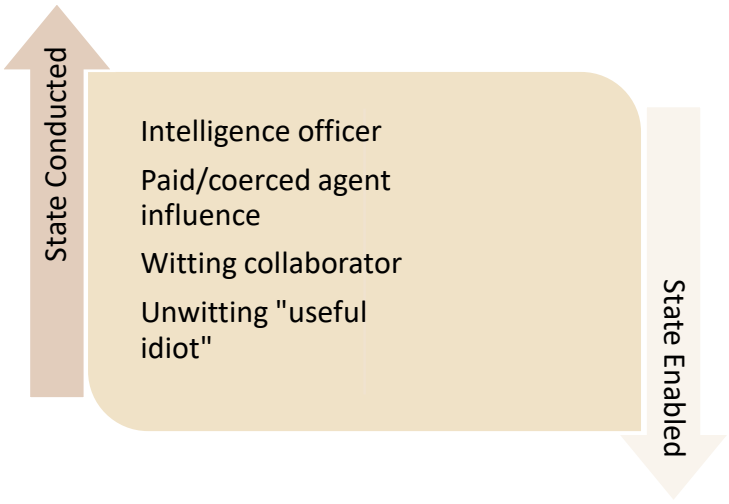

Fig.3.1 Mapping State Involvement

3.4.1 Individuals

States benefit from the support of the following actors:

i) Those directly employed by the state, such as **intelligence officers**, are most likely to be involved in state conducted operations.
ii) **Agents of influence** – paid or coerced by the state – also map onto more direct state involvement. However, even a paid agent of influence does not necessarily equate to state control of that individual.
iii) Moving further down towards state-enabled operations, states work with **witting informal collaborators**. These individuals are already operating independently in a manner favourable to the state and so require light coordination in a manner which advances both their interests and those of the state.
iv) Finally, unwitting so-called **"useful idiots"** are unaware of how a hostile state is benefiting from their actions and ignorant of the hidden hand supporting their carer from a difference.

3.4.2 Organisations

This spectrum of actors equally applies at the organisational level. For example, states have used front organisations in a similar manner. These might be a front organisation directly controlled by undercover intelligence officers or run by paid agents, or they might be technically independent but lightly coordinated from afar. Various Soviet front organisations, such as the World Peace Council and World Federation of Democratic Youth constitute well-known Cold War examples.

This spectrum applies to commercial enterprises. Some firms are state-affiliated or -linked (sometimes discreetly), thus providing these firms with a competitive advantage but also allowing them to interfere in the marketplace, beyond espionage and with potential to impact outcomes. For example, a state might discreetly support a company to impact ICT supply chains by dominating raw earth materials or 5G infrastructure in foreign states. Alternatively, an intelligence agency might use an ostensibly commercial company as a front to hide intelligence activities. The Civil Air Transport is a well-known example of a CIA front from the early Cold War.

3.5 Exposure, Acknowledgement and Secrecy

Political and economic interference can be conducted overtly, covertly, or anywhere in-between. Activity can be unexposed but unacknowledged, exposed but unacknowledged etc. depending on the state's objectives, attitudes towards risk, and ability/willingness to ride out political criticism. See figure 1.2, *Scales of Exposure and Acknowledgement*, above.

Most subversive statecraft activity is discreet, if not necessarily entirely secret. Approximately 80% of malign finance in the West is legal, reliant on loopholes. It is discreet, complex, and not proactively acknowledged – but it is traceable. Discretion allows leaders to avoid accusations of political meddling and allows the beneficiary to avoid accusations of being a stooge for a foreign power. It is rare for either actor to have sufficient clout to get away with accusations of meddling.

Secrecy comes at the price of impact. Activity which is plausibly deniable, and results in minimal exposure, operates beneath a certain threshold. It is difficult to engage in sufficient activity to make a significantly consequential impact if that activity must remain undetected.

Degrees of exposure vary. Some exposure can signal resolve and/or construct myths about power and capabilities. It can undermine trust/confidence, intimidate voters, or spread paranoia. Many Russian operations for example, such as the 2016 Montenegrin coup attempt, are implausibly deniable, but this can still bring benefits.

Even so, **acknowledgement of subversive statecraft is unlikely**. Acknowledgement gives unnecessary ammunition to political rivals, draws political criticism, and invites a response.

3.6 Impact and Success

3.6.1 Regime change: Electoral Interference

States have a greater chance of success when operating overtly, as it allows them to break the secrecy threshold and generate a larger swing to the favoured candidate. However, given the risks of political blowback, more historical examples exist of success when operating covertly.[21]

Propaganda is the most straightforward means of interfering in an election, with states able to achieve widespread reach through use of inauthentic social media accounts etc (see Chapter 2). However, turning this into a change of voter behaviour amongst swing voters, rather than reinforcing existing beliefs in an echo chamber, is much more difficult. **Successful reach does not equate to successful impact**.

Directly manipulating votes is the most impactful means of electoral interference, but it is the most difficult to achieve. Gaining illicit access to election infrastructure is hugely challenging given protective security measures and de-centralisation of infrastructure. Importantly, the narrative around such activity is more consequential than the (often limited) outcome in so far as it casts doubts about the sanctity of results.

Even so, **rigging elections is the most successful means of covert regime change**, at least in the short-term. This is because democracies have freedoms (of the press, opposition parties, movement, dissent, grassroots protest etc) which can be exploited by hostile intelligence agencies.

[21] Dov Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results', *International Studies Quarterly*, 60/2 (2016): 189-202.

3.6.2 Regime Change: Coups

Coups are even more difficult to achieve. Targets need to have a modern, self-functioning bureaucracy which can be detached from the political leadership. The armed services, intelligence agencies, police and professional civil service can then continue to function in the same way as before, but under new leadership. Yet if the machine is too well organized or sophisticated, with discretion to identify what is appropriate and what is not, as in the US, Australia, Germany, and the UK, then a coup becomes unlikely.

Alternatively, if the machine is too closely tied to a single party or leader with decades of practice in coup proofing, then success is equally unlikely.

Coups work best in states:

- With an **apathetic population**, or one which actively distrusts the government.
- Where the average citizen is **economically or educationally deprived** and cut off from wider politics outside of their immediate community or is more politically literate but sees their taxes spent on the lavish lifestyle of the elite.
- Where **power is held in the centre** by elites.
- Which are **politically independent**, for example the 1956 coup in Hungary was unlikely to succeed due to Russian dominance.[22]

3.6.3 Regime Change: Economic Sabotage

Economic measures to force regime change are unlikely to succeed. They can only ever work alongside a range of other measures. For example, in the 1960s, the US supported a general strike in British Guiana designed to remove the prime minister. Crucially, it complemented overt support and a wider range of covert actions from propaganda to electoral interference.

Such activity is less likely to succeed today given the interconnected nature of the global economy. Covert economic influence at a scale large enough to change a regime would a) not be especially covert and b) have ramifications for the benefitting state and its allies.

3.6.4 Longer-Term Effects

Successful covert regime change does not necessarily bring longer term success. Recent research indicates the following consequences:[23]

- **Electoral interference decreases levels of democracy in the target state**.
- **Covert regime change does not bring about longer-term alignment of interests, as measured trough UN voting patterns**. The new leader has two principals: his/her domestic population and well as the benefiting state, thus leaving them subject to contrasting pressures and to the same internal constraints as their predecessor.
- In the Cold War, **US covert regime change operations increased the likelihood of armed conflict** between the US and the target state by about six times in the decade afterwards. Even a successful regime change did not decrease the chance of conflict: it stayed the same as it would have been had the US not undertaken the operation at all. When it failed, however, the risks rose considerably.
- **An increase in instability, violence, civil war, and mass killings**. Ousted governments might disperse to the countryside and launch an insurgency against the new regime.

[22] Luttwak, *Coup d'Etat*.
[23] See Dov Levin, *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions* (Oxford University Press, 2020); Lindsey O'Rourke, *Covert Regime Change: America's Secret Cold War* (Cornell University Press, 2018).

3.6.5 Below Regime Change

Most political and economic actions do not aim to overthrow a regime; they have far more intangible goals. Impact is therefore less dramatic – and less obvious – but more pernicious. To remain plausibly deniable, the impact or intensity must remain below the visibility threshold.

Measuring success is difficult. Such operations do not start from scratch, but rather support existing factors and causes. **It is difficult to separate the agency of the hidden hand from internal forces**. Often observers conflate correlation of objectives and outcomes with impact. Likewise, separating the impact of covert influence from open diplomacy is equally difficult.

Impact becomes subjective and, to an extent, constructed. Overplaying the hidden hand can distort political debates or academic freedom in its own right, by, for example, leading to self-censorship. **The hostile beneficiary state and the target have incentives to collude in the fiction of potency**. For the beneficiary, it makes them appear powerful and able to meet objectives set by policymakers; for the target, it provides a useful scapegoat to explain, for example, successive electoral defeats. States facing political divisions have an incentive to accuse dissidents and hostile states of subversion to mask their own problems.

Policymakers and commentators therefore need to think carefully when exposing and describing covert political influence operations.

4. Paramilitary Influence

Paramilitary activity has both violent and political effect. It subverts targets, creating pressure which can be exploited. Disruption and signalling constitute far more common aims than more ambitious objectives such as regime change, defeating a terror group, or outright military victory in a proxy war. Paramilitary activity consists of proxy wars, sabotage, and assassination / targeted killing. All three can be conducted overtly and covertly depending on the aims and risk appetite of the state. Paramilitary activity is an enabler. It struggles to achieve strategic effects on its own but must be combined with other forms of political and military activity. Trade-offs exist between secrecy, control, and impact. States cannot operate secretly, maintain control, and generate significant impact.

4.1 Introduction

Paramilitary activity includes waging proxy wars, sabotage operations, and assassination / targeted killing. **It sits at the more violent, visible, and risky end of the spectrum but remains a form of subversive statecraft**. In an era of so-called hybrid warfare, cuts to military budgets, and states feeling emboldened to act with greater impunity, such activity will continue even as deniability becomes harder to maintain. It sits between war and peace, but can also complement conventional inter-state military activities, whilst also being prevalent in counterterrorism and in the multiplicity of civil wars across continents. **Cyber capabilities offer new routes to conduct such activities, from AI-assisted assassination to cyber-sabotage, but do not transform the fundamental strategic purpose and principles of each**. Putting the cyber dimension into the wider historical and conceptual context ensures that leaders do not overestimate its effects nor forget hard learned lessons.

4.2 Proxy Wars

Proxy wars are the indirect engagement in a conflict by third parties wishing to influence its strategic outcome.[24] They are constitutive of a relationship between a benefactor (who is a state or non-state actor external to the dynamic of an existing conflict) and their chosen proxies (who are the conduit for weapons, training, and funding from the benefactor).

Such arms-length interventions are undertaken ostensibly for reasons of **maximising interest**, whilst at the same time **minimising risk**. In short, proxy wars are the logical replacement for states seeking to further their own strategic goals yet at the same time avoid engaging in direct, costly, and bloody warfare.[25] Historically, states have exploited specific localised events (such as a civil war) to force a shift in the wider geo-political environment (such as the stifling of a rival ideology in the broader region).

4.2.1 Aims and Appeal

Proxies appeal because they ostensibly minimise risks to the benefactor. Risks include domestic political constraints (i.e. a political backlash from a war weary public opposed to 'boots on the ground' and the combat deaths it generates), economic costs, and risk of military escalation. Proxy wars occur when states or non-state actors, based on a perception of interest, ideology and risk accept that direct intervention in a conflict would be unjustifiable on grounds of cost, illegitimacy, or feasibility.

States support proxies for a variety of reasons including, but extending far beyond, trying to ensure that the proxy force achieves outright military victory. These include:

[24] Andrew Mumford, *Proxy Warfare* (Polity, 2013): 1.
[25] Chris Loveman, 'Assessing the Phenomenon of Proxy Intervention', *Conflict, Security and Development* 2/3 (2002): 30.

- To **overthrow a government** by supporting rebel fighters. This is an incredibly high bar, with few examples of success (e.g. 1980s CIA operations in Afghanistan and Chad).
- Putting **pressure on a target government** by a) creating a costly stalemate and/or b) gaining leverage over a rival by decreasing support in return for concessions.
- **Subverting a target state** by using rebels to weaken a target state's authority. Supporting fighters can a) eliminate the presence of the state in rebel-held areas by, for example, intimidating or assassinating bureaucrats; b) create no-go zones, complete with parallel institutions, raising the cost of governance for the target state and draining resources; and c) create ungoverned spaces to serve as a buffer zone to protect the beneficiary from the target.[26]
- **Signal preferences or communicate resolve** to the target state, whilst the lack of acknowledgement reduces pressure on the target to retaliate compared to an openly declared assault.[27]

4.2.2 Actors: Indirect Influence

Any subversive statecraft that hiring proxies achieves stems precisely from the *indirect* interference they can produce. Direct interference constitutes a third-party intervention (deploying troops or undertaking airstrikes with national military resources, for example). It represents a different mode of conflict given that the state demonstrates a willingness to pay a blood price for achieving a strategic objective by putting its own troops in harm's way. A proxy war strategy, on the other hand, circumvents this age-old moral risk of war.

However, engaging proxies brings dilemmas about how to manage actors which have their own agency, interests, and capabilities. Proxies have independent sources of intelligence and better knowledge of the theatre, thereby giving them the capacity to outmanoeuvre the beneficiary. This is even more the case if the beneficiary is operating covertly and so lacks the ability or presence to monitor the proxy effectively. **The relationship does not equate to control or even sponsorship of the proxy**. It is two-way traffic.

There are four identifiable types of relationships between beneficiaries and proxies that shape the dynamics of proxy wars. These are when:

i) A state uses another state, e.g. US use of South Vietnam as a proxy.
ii) A state uses a non-state actor (such as a terrorist organisation, militia group or private military company), e.g. Hizballah in Lebanon.
iii) A non-state actor uses a state, e.g. Hizballah in Syria.
iv) A non-state actor uses another non-state actor, e.g. Lashkae-i-Taiba (Le-T) & Al-Qaeda.

Although superpower states have used the strategy of war by proxy to the largest effect, smaller powers have also attempted to indirectly intervene in conflicts outside their own borders, notably in the Horn of Africa.

4.2.3 Covert *and* Overt

Proxy wars do not necessarily have to be conducted covertly, but they rest on an underlying premise of *indirect* direct engagement, with, for example, State A hiring proxies in State B to conduct 'subversive operations' for them. Intelligence agencies and special forces personnel of course play roles in the prosecution of proxy wars, but this is only in a training and advisory capacity. Supporting a proxy openly can be a form of power projection. The subversive element of using proxies lies in the indirect nature of the use of force.

[26] Melissa M. Lee, *Crippling Leviathan: How Foreign Subversion Weakens the State* (Cornell University Press, 2020).
[27] Auston Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton University Press, 2018).

4.2.4 Mechanisms of Subversive statecraft

There is not one uniform way in which proxy wars are fought. Means include through providing:

i) **Manpower**, whether bolstering the number of 'boots on the ground', via a surrogate force or non-combatant military 'advisers'.
ii) **Materiel**, such as arms, ammunition, and other military technology, is the prime way for benefactors to get others to do the fighting for them and thus achieve influence.
iii) **Financial assistance**. For example, one estimate of total Soviet financial provision to 'Third World' proxies (*excluding* its foremost proxies in Cuba, Vietnam and North Korea) between 1955 and 1980 puts the figure at around $51billion.[28]
iv) **Non-military means**. A proxy might seek a benefactor's help because of the attractiveness of their political worldview, or indeed a benefactor emphasising the appeal (or legitimacy) of their ideology as a source of attracting allies in strategically important areas. Alternatively, non-military assistance might involve influence operations and/or information warfare to win hearts and minds of local populations (see Chapter 2).

4.2.4 Impact and Limitations

Supporting proxies, especially covertly, to achieve an outright military victory is rare. Secrecy puts a ceiling on success and impact. The more indirect a state seeks to be, to increase plausible deniability, the less control it has over the proxy and the less impact it achieves. Maintaining stalemate and draining the adversary's morale and resources constitute more likely outcomes.

Even lowering the bar for success to include signalling, disruption and subversion still does not leave proxy wars a risk free or straightforward option.

i) First, proxies have agency of their own. They are difficult – if not impossible - to control and may **outmanoeuvre the beneficiary**; interests may only temporarily align, and proxies can eventually outgrow or even turn on the beneficiary. Alternatively, supporting a proxy with values antithetical to those of the beneficiary, i.e. if a liberal democracy supports a terrorist organisation, can create embarrassing political repercussions if exposed.
ii) Second, whether these proxy interventions are undertaken between the US and China in Africa, by myriad states in cyberspace, or by PMCs in the developing world, indirect interference in existing conflicts may reduce conflict escalation, but it risks **conflict intensification**. They may circumvent the potential international political uproar at a direct intervention, but they do increase the chances of **higher casualties** as a result of the influx of externally sourced weapons, money or personnel.
iii) Third, they also run the risk of creating longer-term **dependency** between the proxy and the benefactor in a post-conflict environment.[29]

[28] Steven R. David, 'Soviet Involvement in Third World Coups', *International Security* 11/1 (1986): 7.
[29] For further discussion of the consequences of proxy warfare see Andrew Mumford, 'Disarmament, Demobilisation and Reintegration (DDR) After Proxy Wars: Reconceptualising the Consequences of External Support', *Third World Quarterly* (published online September 2021) DOI: 10.1080/01436597.2021.1981762.

Case study: China and the use of proxies

The rise of China as a global power has provoked consternation in the West as to how it will reconcile its inherent inwardness with new-found inclinations towards international economic and political influence. China's reliance on economic expansionism may avoid a Cold War-style superpower stand-off, but it instead raises a different prospect of a global power shift as a result of China maximising *indirect* uses of its power to secure long-term interests (both economic and political) whilst reducing the risk of war with the US.

China's long-standing foreign policy 'golden rule' of non-interference in the internal affairs of other countries will be severely tested as the Chinese Communist Party (CCP) seeks ways to maintain high levels of economic growth with limited amounts of domestic natural resources and an expanding population.

China's current access to African oil, cobalt, gold, copper and iron ore may well be constrained in the future by competitor states or internal disruption to supply (through civil war, for example). Two of the main catalysts to proxy wars identified in this chapter – interest and ideology – are compounded in the Chinese case given the very nature of their one-party state.

Furthermore, the issue of risk management is all the more acute in China's case given the huge economic stakes involved in its new power status. Talk of China's peaceful rise to the status of global superpower needs to be heavily couched in terms that closely scrutinise China's *indirect* forms of power projection and interest maximisation. Indeed, it could be argued that a form of proxy warfare has been simmering between China and the US for some time now, with the Americans using Taiwan as a regional surrogate to block expansions of Chinese military power.

4.3 Sabotage

Sabotage is often associated with wartime special operations: blowing up Ottoman railway lines or Nazi heavy water plants. States continue to employ sabotage today as a means of subversive statecraft. It can take place online and/or offline, and it is important to overplay neither the novelty of the cyber dimension nor the distinction between the two realms. **Cyberattacks are a modern manifestation of centuries old practice of damaging, destroying and degrading targets**.

4.3.1 Aims and Appeal

Whether conducted online or offline, aims are often the same: to disrupt, delay, degrade, and frustrate the adversary.

Sabotage is a force-multiplier. It can soften the ground to allow friendly forces to do their jobs more efficiently. For example, Russia used covert sabotage teams to lay the groundwork before military operations targeting Georgia and Ukraine. In 2022, Ukrainian special forces teams allegedly conducted sabotage operations, including arson, inside Russia in order to disrupt the Russian war effort and multiply the effect of Ukrainian defence.

Sabotage also has psychological value. It – and even just the threat of sabotage – can lower morale. For example, Western sabotage of ISIS equipment not only degraded the group's capabilities, but also induced paranoia and encouraged mistakes. (See also section 2.6 above on propaganda of the deed.)

Sabotage appeals to states because, like proxy warfare, operations offer a light footprint, obviate burdens of victory, and disrupt hostile actors before they can attack.

4.3.2 Delivery and Targets

Sabotage seeks to achieve strategic effects from (a series of) individual strikes. Targets therefore include those likely to do most damage beyond the immediate and which can be exploited by other arms of the state: supply lines, fuel pipelines, critical national infrastructure, transportation networks, banking and governance systems, communication and internet networks, and weapons production.

Traditional means of explosives, delivered by special forces, proxies or even drones remain prevalent. For example, Iran and Israel have engaged in a shadow tit-for-tat sabotage against tankers and ships in the Gulf using explosives since 2020.

Cyberattacks also sabotage targets. This is often combined with analogue or real-world activity, and it is a mistake to treat them as mutually exclusive. For example, Israeli sabotage of the Iranian nuclear programme has involved a combination of the two.

Like proxy warfare, **cyberattacks are subversive**: persistently exploiting vulnerabilities to undermine authorities from within. Attacks exploit weaknesses and manipulate targets. They destabilise, undermining their ability to function as intended. Cyberattacks subvert computer systems to orchestrate political, physical, and economic effects. **Cyber conflict is intelligence conflict, with ambiguity at its heart**.

Case Study: Stuxnet

The Stuxnet cyberattack on Iranian nuclear capabilities, uncovered in 2010, highlights three important points. First, cyber capabilities can inflict physical sabotage (in this case of centrifuges). Second, even though cyberattacks theoretically reduce risk by allowing states to operate remotely, human agents are still involved (in this case an engineer inside the plant). It is therefore important not to overplay the online/offline distinction. Third, the success of the operation is contested, despite meeting its immediate objective. Critics claim that it did not retard the programme in any meaningful manner and, worse, may have increased suspicion between Iran and the US thereby making diplomacy more difficult. The exact contribution of the covert action to the 2015 nuclear agreement is unknowable.

4.3.3 Impact

Sabotage cannot deliver a decisive blow; it is unlikely to make a difference on its own. Instead, it is disruptive and subversive, wearing down the enemy by persistently targeting key vulnerabilities or symbolic targets. It is a force multiplier to be used judiciously to generate strategic effect.

Cyberattacks are unlikely to achieve mythologised "cyber 9/11" effects. First, any such devastating sabotage would not be a single out-of-the-blue attack. Second, governments have little incentive to advertise the effects of any such attacks. Third, high-value targets pose greater risk and costs to those that that them, through defensive measures including deception operations which can reduce confidence.[30]

Cyberattacks are subject to the same trade-offs as other forms of subversive statecraft.

[30] Eric Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security* 38/2 (2013): 41-73.

- Secrecy is important because if the attack is inadvertently exposed, the target can patch vulnerabilities. Yet secrecy and the subsequent desire to act indirectly put a ceiling on activity, while also limiting speed.
- Increasing the scale of attacks decreases the speed, the secrecy and control. The wider the scope of targets and bigger the scale of the attack, the more likely the state is to be detected. The more control, the less deniability.
- Being more indirect, and thus more secret, leads to less control. Outsourcing to private hackers risks unauthorised activity.[31]

4.4 Assassination and Targeted Killing

Killings of targeted individuals, particularly terrorist leaders, increased dramatically since 9/11. Israel had earlier paved the way for such activity, extending to Iranian nuclear scientists, but the USA quickly followed suit. Notable American strikes include on Al Qaeda leaders, Osama bin Laden, Anwar al-Awlaki (2011), and Ayman al-Zawahiri (2022), and on Iranian general Qasem Soleimani (2020). Use of drone strikes has since proliferated globally, with states including Turkey and Nigeria using Chinese and Iranian made weaponry.

Authoritarian states have recently engaged in a series of high-profile attempts to assassinate dissidents and journalists. This includes the Russian assassination of Alexander Litvinenko (2006) and attempted assassination of Sergei Skripal (2018); the Saudi assassination of Jamal Khashoggi (2018); and the North Korean assassination of Kim Jong-nam (2017).

Such activity will increase so long as norms against targeted killing erode and as authoritarian states get away with assassinations.

4.4.1 Aims

States kill targeted individuals for a variety of reasons beyond simply neutralising an imminent threat. Countering or responding to such activity therefore requires a sophisticated understanding of objective. Objectives include:

- To **disrupt and reduce** the technical expertise of adversaries (such as Iranian scientists or terrorist bomb makers) which is difficult to replace.
- To **send a message**. For example, the attempted assassination of Sergei Skripal in 2018 sent messages to multiple audiences: warning defectors and would-be defectors that they can be targeted; warning British counterintelligence not to harbour or recruit Russian dissidents; demonstrating the performative power of Putin as a strongman leader both to the west and to the domestic population.
- To **change a regime** (this is unlikely to succeed, see 4.4.3 below)

4.4.2 Means, Directness, and Secrecy

Like all forms of subversive statecraft, state involvement in targeted assassinations exists on a scale of directness (see fig. 4.1 below).

The most direct approach allows states to **use their own forces – paramilitary, drones, intelligence, or special forces – to remove a target**. See, for example, the US drone strike killing the Iranian general, Qasem Soleimani in 2020. A direct strike leads to greater control and greater chance of success, but at the cost of secrecy.

[31] Lennart Machsmeyer, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security* 46/2 (2021): 51-90.

Paid agents, recruited by an intelligence agency and tasked with killing a target, are slightly less direct. Further down still, the agent might be unwitting, as appeared to be the case with the North Korean assassination of Kim Jong-Un's half-brother in Malaysia, 2017.

Next, intelligence agencies can supply a group with weapons – but issue no orders and ask no questions. It **facilitates** something likely to happen anyway.

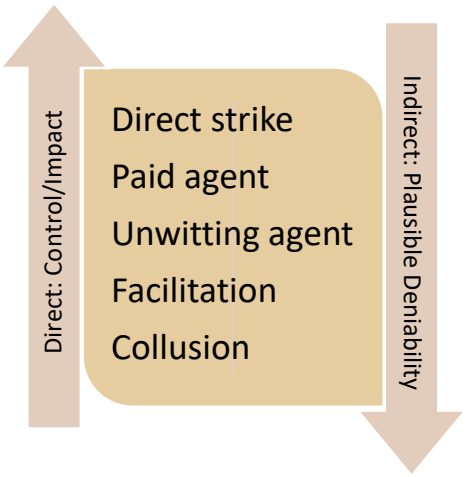

Fig. 4.1 Scale of Directness

Finally, **states collude with violent non-state actors**. This might be as passive as simply turning a blind eye to terrorist activity or not investigating crimes properly, as was the case with the UK government in Northern Ireland during the Troubles. Collusion renders it difficult, if not impossible, to prove the hand of the state in a killing. However, the state has little control over violence.

This scale of directness, and the trade-offs involved, mirror fig 3.1 in Chapter 3 mapping state involvement. **Understanding the relationship between state and the individual conducting the killing is vital to counter this activity**.

4.4.3 Impact and success

Targeted strikes against state leaders are rare, illegal, and unlikely to succeed. They are especially unlikely to result in regime change: the strike would both have to succeed in killing the individual target *and* in bringing about a friendlier alternative. A rare example of success comes from the Soviet assassination of the Afghan president in December 1979. Special Forces successfully killed him (at the second attempt) but only managed to replace the regime with a friendlier alternative by combining the assassination with an overt miliary invasion on the very same day.

States enjoy more success at a less ambitious level. This includes Russian killing of dissidents overseas, such as Alexander Litvinenko; Israeli killings of Iranian nuclear scientists; and US killings of terrorists from Somalia to Pakistan.

An operational or tactical success does not necessarily translate into cumulative impact and strategic success. Subversive statecraft at the strategic level is more difficult to measure. Too often, policymakers and academics determine success by the number of people killed because it is an easier metric, but it is ultimately misleading.

Failure to kill a target might not necessarily be a strategic failure. The botched Russian operation to kill Sergei Skripal succeeded in sending a message to other dissidents, would-be dissidents, and to MI5.

Successfully killing terrorists might be counterproductive in the longer term. It can normalise targeted killing; radicalise others, perhaps leading to a less restrained membership of a terrorist group; and does not necessarily make the collapse of a terrorist group more likely.[32]

[32] See Jenna Jordan, 'When Heads Roll: Assessing the Effectiveness of Leadership Decapitation' *Security Studies* 18/4 (2009): 719-55.