Just Spying: Defending the Legitimacy of Covert Action as a Means of Diplomacy

Dr Brendan Walker-Munro, PhD

Law and the Future of War Research Group, T.C. Beirne School of Law, The University of Queensland

b.walkermunro@uq.edu.au

Spying is often referred to as the second oldest profession – yet the lawfulness of the employment of covert actors to achieve diplomatic and foreign policy objectives in a peaceful fashion has received patchwork attention from academia. Under both international and domestic legal frameworks, the covert acts of agents of a State are essentially unregulated, with espionage charges only attaching to the actions of a spy if they are caught, though sanctions may apply if the actions were attributable to their hosting nation. The obvious value of covert action remains the achievement of diplomatic and foreign policy objectives which cannot be secured by conventional means, and for which armed conflict is an unacceptable or unlawful recourse.

This paper will critically examine the international and domestic treatment of three commonly employed forms of covert action by States: information operations, pre-emptive "strikes" and cyberattack or cyberwarfare. The specific methodology of each case study will be examined in detail and compared to both international and legal frameworks which might broadly apply to such conduct. These case studies will be used to present the argument that actions taken on a covert basis in furtherance of peaceful diplomatic or foreign policy should receive broader international and domestic legal protection to incentivize its use over armed conflict.

Keywords: covert action, lawfare, legitimacy, international law, comparative law, spying

 ISBN: 978-86-87043-84-8

Just Spying: Defending the Legitimacy of Covert Action as a Means of Diplomacy

History and experience prove that foreign influence is one of the most baneful foes of republican government…

--President George Washington (Mohan & Wall, 2019, p. 116)

Introduction

Anecdotally, spying is considered the second oldest profession. Sheldon (1997) and Perley (2016) makes convincing arguments that site some of the first acts of organized spying inside the Roman Empire, gathering information and evidence during both the expansion and fall of that mighty empire. Sun Tzu concisely detailed the "five classes of spies" and gave well-explained and considered strategies for their employment for rules in the 16th century (Giles, 2005, p. 86). Machiavelli – in a work published at the same time as Sun Tzu's and somewhat ironically called *Art of War* – made clear and frank references to the use of spies both in war and peacetime (Evans, 2014). Spying is even suggested to have occurred during the conflicts of the Old Testament (Frolov, 2007).

One of the unifying themes of these early scholars was the notion of individual agents, acting at the behest of a broader regime or government, yet seeking to influence local, regional or strategic outcomes. Often these acts involved brokering agreements, solving disputes or otherwise resolving matters which could not be dealt with using traditional methods of diplomacy between States (Stempel, 2007). Another similarity of these early works was a lack of discrimination between what we might now term individual acts under the umbrella of the term "spying". Ironically, despite the amount of time that humanity had to perfect the practice, the entire domain of activities we might refer to as falling within the domains of spying appears under-theorised as both a concept of international and domestic law, but also of international and foreign relations (Andrew, 2004).

A more nuanced analysis of the actions that constitute "spying" yields a list of activities that involve different methodologies and tactics, and carry vastly different legal, moral and ethical ramifications for their conduct – consider the significantly divergent treatments and opprobrium associated with acts such as espionage[1], sabotage[2] and assassination.[3] There are also other actions of State agents which do not necessarily involve the application of kinetic or lethal force, or which do not seek to place a State at its own detriment. It is only right and proper therefore that we should start with a more concise definition and typology – one that displaces "spying" and its associations, both positive and negative (Fabre, 2022) – with a more nuanced term.

Collectively then, this "third way" of foreign relations comprises those actions open to a State that lie between, and at the edges of, open warfare and traditional diplomacy (Johnson, 2020; Johnson, 2021). In the literature this third way is described as <u>covert action</u>, a phenomenon which has significant utility in securing peace and resolving diplomatic conflict. Covert action is generally understood as those activities of a State's agents which influence conditions abroad and where it is intended that the

---

[1] Defined as "acquiring secrets held by another… in conditions where the person with the secret may go to extreme and often violent means to prevent their secrets being compromised" (Omand and Pythian, 2022, p. 40).
[2] Defined as "the destruction of property to gain a definite, revolutionary, [or] economic end" (Walker C. Smith, 2004).
[3] Defined as "an act of killing a prominent person selectively, intentionally, and for political or religious purposes" (Kasher & Yadlin, 2005, p. 44).

role of the State will neither be apparent nor acknowledged publicly (Johnson 1989, p. 18). Such a definition is enacted in legislation in certain States to provide guidance to the acts of the relevant government agents – this definition of covert action as influencing conditions abroad in a secret or non-attributable manner appears in 50 U.S. Code, §3093e (Warner, 2019, p. 34).

Alternately, covert action may be defined as intervention in the internal affairs of another State or non-State actor in an undetectable or plausibly deniable manner (Cormac, Goodman and Holman, 2016, p. 14). If a covert operation goes undetected then its sponsoring State will not be revealed; however, if the operation fails or is detected, the nature of the action should be such that the sponsoring State still has plausible deniability in respect of that action (Joseph and Poznansky 2018, p. 322). Again, the United States (US) statute books carry a description of utility to this article: the *United States Intelligence Authorization Act 1991* described covert action as activities "…to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent of acknowledged publicly" (US. Congress.gov, 2022).

For this article, I intend to approach the inquiry using the definition supplied by Warner (2019, p. 33): "Covert action is the secret supplement to war and diplomacy, employed at the margins of conflict to shift patterns of trust and allegiance". This definition has a series of benefits – firstly, it acknowledges the secrecy of the conduct, but that it sits alongside and adjunct to traditional methods of warfare and diplomatic negotiation. Secondly, this definition also recognizes and places inquiry on the purpose of covert action, which is to alter concepts like trust and allegiance in ways that are beneficial to the sponsoring State. Thirdly, this definition also enshrines the concept that covert action is relatively target-agnostic; that is, the action may be directed at an individual or a class of individuals, or at a State or non-State actor – what matters is the purpose of that action in shifting patterns of trust and allegiance. Lastly, it removes from the definition of covert action certain conduct which I consider to be unpalatable in the context of diplomacy: that of regime change. Actively seeking to undermine the government in place in a democratic State is – in the author's view – an indefensible and unlawful act of interference with sovereignty (Enterline & Greig, 2008, p. 885; O'Rourke, 2018, p. 53; O'Rourke, 2020, p. 105) and leads to increased risk of conflict (Peic & Reiter, 2011), thus will not be considered further.

Defining Characteristics of "New" Covert Action

For the very reason of its secrecy and deniability, covert action has long been a controversial tool of international relations (Johnson, 2021). But traditional methods of covert action – those perhaps popularized in the Cold War – are no longer fit-for purpose in a digitized environment. Intelligence agencies and their agents are having to adapt to new technologies which offer both new opportunities but also greater risks of detection and compromise. In just two examples, "[t]he proliferation of cell phones with cameras and high-speed Internet to the far corners of the world means that there is always a high risk that evidence [of covert action] will be recorded" (Joseph & Poznansky, 2018, p. 333).

The world has changed. Radsan (2009, p. 487) may have been right to say "[t]he world is so dangerous after 9/11 that it would be irresponsible, perhaps insane, to suggest that our intelligence agencies… should be disbanded. The question is not whether we should engage in covert action, but how often and under what circumstances". Abstinence is no longer good public policy – in addition, technological change, increased public involvement and scrutiny, and concepts of international law and custom are all things that have contributed to a need not to ban or outlaw, but to rethink how covert action is undertaken and under what circumstances. What then might be said about the "new" covert action?

Covert Action is a Technologically-Sensitive Spectrum

If covert action occupies the "third way" between traditional and overt diplomacy, and armed conflict or warfare (Johnson, 2021), then by its very definition covert action covers a wide swathe of State conduct. Undercover agents producing and delivering propaganda, stealing military or commercial secrets, foreign interference of elected officials, bribery, hacking, sabotage – all the way up to the surgical use of force by special military or paramilitary forces in a deniable fashion may constitute covert action. The US, often one of the most scrutinized jurisdictions in the world of covert action, demonstrate the significant breadth of their position on covert action in their *National Security Directive 10/2 of 18 June 1948* (Andrew, 1995, p. 173), which directed and authorized the Central Intelligence Agency (CIA) to engage in:

> …propaganda; economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-Communist elements in threatened countries of the free world.

Of course, covert action can mean different things to different States. For example, some democratic States (such as the United Kingdom and Australia) consider covert actions undertaken by specialist military forces are in fact "special operations" under the imprimatur of the sponsoring State's military prerogative. Because they can lack a specific diplomatic need, these States do not consider special operations to qualify as covert action (Urban, 1992; Stoltz, 2022, p. 7) To other States (such as Russia, US and Canada) the use of military forces in a covert or plausibly deniable manner remains covert action within their legislative framework (Kalugin, 1994; Zegart, 2022, p. 173-174). Yet such distinctions seem entirely fluid dependent on circumstances – for example, the US was more than willing to admit that its special forces soldiers killed Osama bin Laden in Pakistan in 2011 (Wall, 2011). That action was neither covert nor plausibly deniable!

Consider an example to which I return later in this article: the covert use of drone strikes. The US – a State with perhaps the heaviest reliance on drones as a plank of foreign policy – recognized relatively early on that the use of drones in the absence of a declaration of war from Congress might be a breach of international law (McNeal, 2009; Wall, 2011, p. 93). Rather than cease the practice, the determination was that effective control of drone strikes would be taken out of the hands of the special forces (as a military operation) and put in the hands of contractors to the CIA (making it an intelligence operation): effectively, relying on a separate legislative authority to engage in the same conduct (p. 485-486). A use of drones for military purposes would also likely trigger the "military" dimensions of jurisdictions like the United Kingdom and Australia, taking the conduct out of the realms of covert action, but staying well in the bounds for other States.

Covert actions are often Legitimate, but not always Lawful

Closely aligned to the nature of covert action as existing along a spectrum of activities, it is apparent that the width and breadth of activities which constitute covert action will inevitably cross boundaries between and over legitimacy and lawfulness. To be clear, an activity is "lawful" if it accords with the provisions of international (and where relevant, municipal) law applying to the activity in question. For example, overt diplomacy is almost always conducted under the imprimatur of legality provided by international instruments such as the Vienna Convention.[4] States accused of wrongdoing usually have their diplomats expelled or recalled, rather than engaging in uses of force. States cannot act

[4] *Vienna Convention on Diplomatic Relations*, opened for signature 18 April 1961, 500 UNTS 95 (entered into force 24 April 1964).

contrary to such well-established legal norms or, if they do, they face the almost certainty of retaliation and reprisal. In contrast, an act is illegitimate if – were it to be exposed to public scrutiny, either by other States or the population of the sponsoring State – it would fail to receive popular support. Collectively, covert action "occupies a very murky place in international law that might be characterized as either legal but discouraged, or illegal but not enforced" (Cooke, 2010, p. 609).

If leaders make decisions based on their interpretation of popular support in response to their proposed actions, this includes the taking of covert action against opponents of State interests, even where those opponents are democratic States themselves (Tomz & Weeks, 2013; O'Rourke, 2018; Carnegie, Kertzer & Yarhi-Milo, 2022). In such a way, mass opinion can legitimize the taking of "any steps" which would maintain peace and avoid conflict (Johns & Davies, 2012, p. 5); a position somewhat ill-at-odds with a normative framework where democratic States overtly prioritize respect for their neighbours' and adversaries' sovereignty (James & Mitchell, 1995; Kim, 2005; Downes & Lilley, 2010; O'Rourke, 2018).

The trade-off and apparent value in covert action for leaders, and the source of this popular support, is the prospect of achieving results which cannot be reached through diplomacy alone and "for which warfare is unjustifiable or undesirable" (Stoltz, 2022, p. 9). Actions which go undetected or are plausibly deniable offer the ability for States to achieve influence without threat of repercussion or retaliation (Brown, 2014, p. 411). Covert action can also be a force multiplier: States that lack sufficient financial, political or military capital to exert their will can still achieve strategic outcomes in respect of competing and adversarial States (Her Majesty's Government, 2010). Covert action also allows democratic States – predominantly in the Anglosphere – to undertake influence operations against one another in circumstances where overt actions might be considered diplomatically unacceptable or "distasteful" (Poznansky, 2015, p. 815-818).

Similarly, the nature of modern conflicts in which many democratic States participate necessitates covert action. Non-State actors are rarely interested or invested in long-term or attritional warfare, nor are they parties a State may wish to be seen openly negotiating with (Cormac, Goodman & Holden, 2016, p. 15). Unsurprisingly, this creates both an incentive and prerogative for States to "get ahead of the game" by preventing or disrupting the rise of such non-State actors before they can affect a sponsoring State's interests.

This legitimacy – the popular support of a State in undertaking a covert action – is of course not to be confused with legality. If State sovereignty is defined as "the monopoly of choice"[5] (Schmitt, 2005, p. 13), then covert action involving the manipulation or influence where the sponsoring State is hidden will interfere with the target State's rights of determination and autonomy laid out in art 1 of the International Covenant on Civil and Political Rights,[6] and breaching the custom of non-intervention outlined in *Nicaragua*[7] (Schmitt, 2018; Poznansky, 2019). Despite the seemingly irreconcilable natures of covert action and State sovereignty, so-called "clever lawyers" have justified everything from the invasion of Iraq in search of weapons of mass destruction to the use of special forces to kill terrorists in foreign countries (Keohane, 1997; Sanders, 2011; Perina, 2015).

---

[5] Otherwise defined as "in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State": *Island of Palmas Case (Netherlands v US) (Awards)* (1928) 2 RIAA 829.
[6] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered
into force 23 March 1976).
[7] *Nicaragua v United States of America (Merits)* [1986] ICJ Rep 14.

 ISBN: 978-86-87043-84-8

Covert action is becoming a greater part of public consciousness

The risk of covert action becoming public is also now greater than ever. The public is far more eager to hold governments to account, especially in the domain of covert action and doubly so where the action involves covert use of force (Bovens, Hart & Peters, 2001, p. 21; Carnegie, Kertzer & Yarhi-Milo, 2022). In addition to the greater levels of physical and electronic surveillance in many States, the prevalence of cellphones and high-speed internet increases the likelihood that physical acts of covert action (including planning and preparatory steps) will be recorded and exposed. In fact, empirical studies have linked the likelihood and consequence of exposure of covert action with an increase in the sophistication of the targeted State's telecommunications infrastructure (Joseph & Poznansky, 2018).

Covert action also tends to include broader and more diverse ranges of non-State actors – such as private security contractors – which in turn increases the risk of accidental or deliberate leaks of classified plans, either *ex ante* or *ex post* (Cormac & Aldrich, 2018). Where they do become involved, State actors are often challenged by the new technologies of the worldwide economy (Aldrich & Cormac, 2016, pp. 485-491).

When covert action is revealed (either by scandal or betrayal: Radsan, 2009, p. 521-522), the secrecy attendant with such operations usually allows States to limit both local and global narratives in a way that avoids escalated conflict (Carson, 2016, p. 105). Covert action causes less damage, if leaked, when it is compatible with public opinion (Cormac, Goodman & Holman, 2016). Of course, secrecy of covert action can be something of a double-edged sword – covert action that is disconnected from broader strategic thinking and forms of overt action or those using *ad hoc* and ill-considered approaches, can suffer from criticism and scrutiny at the risk of being labelled "dangerous" or "rogue" foreign policies (Aldrich & Cormac, 2018, p. 18). Further, there is often inadequate consideration of what happens when covert actions become *overt* from the perspective of the sponsor State population as well as of the target State and/or States in a similar position to the country in question (Prados, 2007, p. 290).

The counterpoint to "leaked" covert action ought to be that which is sanctioned by the executive leadership of a State. However, Regan & Poole (2021, pp. 232-248) described how this scrutiny is discharged in two modern democracies by reference to the United Kingdom's (UK) Joint Action Committee (JAC) and the US' National Security Council (NSC), resulting in significant differences. Even between these two trans-Atlantic jurisdictions, the differences are stark: under the UK model, agencies undertaking covert action do not need to notify Parliament, do not need specific legislative authority to undertake their functions and may use special forces "on secondment" without needing to formally transfer military command. Given the significant criticisms of UK's former covert action strategies as being neo-colonialist in nature (Cormac, Walton & van Puyvelde, 2022, p. 124), there is perhaps some ground to reconsider the benefits of scrutiny for covert operations for countries that lack a system with the robustness of the US.

Typologies of "new" covert action

What then, does "new" covert action look like? The answer is not merely *more of the same*, but perhaps more likely to be *same, but different*. Intelligence agencies and (where they are used) their non-State counterparts need to acknowledge and plan for the challenges of emerging technologies, as well as identifying the contours of opportunity that arise from those same technologies. How they may do so will be explained using three case studies of "new" covert action.

Information operations

The term information operations is defined here as "efforts by individuals and groups, including state and non-state actors, to manipulate public opinion and change how people perceive events in the world by intentionally altering the information environment" (Starbird, Arif & Wilson, 2019, p. 2). That definition obviously is amended slightly to take into account the definition of covert action being used in this article, and thus the utility of that methodology to States in seeking to achieve diplomatic or foreign policy outcomes without attribution, or in circumstances of plausible deniability.

The information environment is particularly sensitive to the operations of covert actors: firstly, because of its high reliance upon emerging technologies and systems which allow persons around the world to access and digest online content; and secondly, because of the low cost and ease with which State and non-State actors can establish narratives and counter-narratives which support their broader strategic outcomes. Consider for example the alleged influence in national elections: one analysis of covert actions of the USSR and US between 1946 and 2000 suggests that these two superpowers attempted forms of covert influence on 117 occasions (Levin, 2016, p. 189). This influence is now increasingly being undertaken by sophisticated electronic capabilities on behalf of States and has occurred in at least two Presidential elections, one in the US and one in France (Hansen and Lim, 2019). From a legal perspective, information operations occupy a unique position in the lacuna of international law: where actions are taken that interfere (for example) with elections as a process of democracy, it would seem logical that these actions would constitute an unacceptable violation of the principles of sovereignty and non-intervention. But that legal position is far from easily explainable.

Firstly, the very practice of information operations on a covert basis does not *prima facie* violate any treaty or instrument of international law, save the non-interventionist principles in Article 2(4) of the UN Charter. However, many scholars have concluded that if information operations are unlikely to achieve outcomes consistent with an "armed attack" and permit self-defence under Article 51, then Article 2 likewise provides little protection from the practice (Damrosch, 1989; Williams, 2011; Hamilton, 2017). Some have even suggested States have deliberately excluded these forms of covert statecraft from *jus ad bellum* and international humanitarian law frameworks to tacitly permit their practice (Beard, 2014, pp. 99, 117-118). Arguments that the conduct of information operations engages Article 2 of the *International Covenant on Civil and Political Rights* (which requires States "respect" the privacy of individual privacy globally) or Article 17 (which prevents arbitrary interference with privacy) are equally unconvincing (Ohlin, 2017, p. 1585). Nor are information operations a violation of customary international law – despite *Nicaragua* – where so many States apparently engage in the practice of interference in the governmental operations of their neighbors and adversaries (Baxter, 2013; Ohlin, 2017, p. 1582; Lahmann, 2020).

Secondly, the right of States to perform their "inherently governmental functions" may not qualify for protection and be free of interference, as the nature of the protection is dependent on all the circumstances of the interference. For example, transmission of propaganda may not be unlawful but inciting unrest or transmitting while using territorial waters for passage may be (Schmitt & Vihul, 2017, pp. 24-26). The release of misinformation and disinformation to sway voters in an election may not constitute interference unless it directly corrupted or maladministered the processes of democratic functioning, being the *domaine reserve* of the government in question (Ohlin, 2017, p. 1594). On the other hand, information operations may constitute an interference with the right to self-determination of the victimized State, because it has intruded on the "right of [the people of the State] to determine for themselves their political destiny" (Ohlin, 2017, p. 1596). Further, large democratic States often choose to sell a narrative that their interference in non-democratic States is for the protection of this same right of self-determination for the oppressed and marginalized – whether that narrative is plausible or not (Coe, 2015).

Thirdly, the very purpose of covert action is to remain either undetectable or plausibly deniable to the sponsoring State. In circumstances where that criterion is met, whom does the international law hold accountable? If information or propaganda is release from a piece of State infrastructure, does that make the State controlling or housing that infrastructure liable for the information or propaganda? Or does the victimized State face the same challenges as with attributing traditional covert actions, with the added difficulty that there may be no physical agent to detain and prosecute (Banks, 2017, p. 1501)?

The solution appears to have been to plug the gaps in international law with domestic or municipal laws which outlaw the conduct of what is broadly referred to as "foreign interference" – the most comprehensive of which was Australia (which passed the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth); Ross, 2022) but have since been followed by other Commonwealth and EU countries such as France (Couzigou, 2019), Canada (Henderson, 2019), German, Israel and India (Haciyakupoglu et al. 2018). For example, the French legislature – which must adhere to European Conventions and Court rulings on human rights legislation – could only outlaw only interference in elections which "objectively false, misleading, and threatens the honesty of upcoming elections… the spread of that information must be artificial or computerized, deliberate, and massive" (Couzigou, 2019, p. 112). Australian law suffers no such limitations, requiring only that the act is undertaken on behalf of a "foreign principal" and the act is intended to influence democratic political rights or duties, support intelligence of the foreign principal or prejudice Australia's national security (Ross, 2022, p. 11).

Yet significant gaps remain: each municipal and domestic law differs on the terminology used to describe the ingredients of each offence, as well as the nature of criminal responsibility (i.e., recklessness, intention, negligence) which must also be associated with the conduct. Thus, what is proscribed in some jurisdictions will be permitted in others – leading to frustration of attempts to prosecute or extradite (Boister, 2018). Further, attempts to define every typology of information operations leads to States questioning the involvement of their adversaries even when no covert action is occurring – whether through confusion or secrecy, the sponsoring State achieves its aims (Cormac & Alrdich, 2018, pp. 486-487).

There also exists significant incentives for States (and non-State actors on their behalf) to engage in information operations under covert action strategies. Information operations can prevent hostility and defuse conflict by agitating public consciousness in directions amenable to the sponsoring State (Gentry, 2016; Jensen, Valeriano & Maness, 2019). These forms of operations can also be linked to covert military activities which seek to "shape" more favorable precursors for more kinetic forms of covert action, equally for the purposes of avoiding future conflict and defusing threats *ex ante* (Madden et al., 2016, p. 144). Achievement of objectives deemed impossible in overt diplomatic circumstances may be possible with the influence or manipulation of the persons or media within a targeted State. Such covert action is also "preferable to overt coercive diplomacy when the coercing state is structurally constrained in either the international or domestic system to gain 'legitimate' approval for the pursuance of coercive measures defined by force against another state", and even more so "if it is used to coerce a state that able to both make concessions and in a decision frame to do so" (Wittmer, 2013, pp. 18-19 and 65-66).

Pre-emptive strikes

Any discussion of covert action in the literature inevitably invokes the US drone program, during which US military pilots (and later contractors engaged by the CIA) controlled drone missions which entered the airspace of foreign countries and executed "precision strikes" on targets deemed worthy of national scrutiny. In the years following the Bush and Obama administrations, during which the drone programs experienced significant growth in size and scale, arguments have continued about the legality of launching such attacks outside the regulatory frame of armed conflict (Wittes, 2014; Perina, 2015; Fuller, 2017; Sanger, 2017; Kibbe, 2022)

From that context, no matter how selective or surgical applications of pre-emptive lethal force might be, it would be strange to suggest they could lead to increased peace or resolution of intra- and international conflicts. However, Mitt Regan's (2022) meta-analysis of both quantitative and qualitative studies into drone strikes against Al-Qaeda supports a notion that whilst the strikes did not achieve the US government's purpose of eliminating Al-Qaeda's leadership, the strikes did prevent widespread organization and planning, as well as "reduc[ing] violence enough to pursue initiatives that could…include local governance and security reforms, and the creation of meaningful economic opportunities, in order to lessen the appeal of extremism" (p. 2). Empirical studies of public responses to covert actions also supports the idea that "while the public dislikes military intervention against democracies in general, respondents prefer covert missions against democracies to overt ones" (Carnegie, Kertzer & Yarhi-Milo, 2022).

This article should not be viewed as an endorsement of the US policy of drone strikes which, at their peak, arguably resembled a State-sanctioned assassination program (Banka, 2017). The piloting of drones into countries which did not consent to the use of their airspace is at the very least a violation of sovereignty and potentially an act of armed aggression (Williams, 2010; Bradley & Nienaber, 2015, pp. 424-425; Forsgren, 2021). Even where States do consent, the power disparity between actors in that transaction create unsavory conditions for "contingent sovereignty" – voidable n the view and at the insistence of the stronger State (Forsgren, 2021).

The legal basis for the US drone strike program was also alleged to be particularly flimsy. States are broadly required by article 2 of the UN Charter to resolve their disputes without recourse to armed attack, unless acting in self-defence. But this protection of self-defence is qualified – no action should be disproportionate to the attack or involve any act whose purpose is "misaligned to the [UN] Charter".[8] Any reliance on the pretext of self-defence under Article 51 of the UN Charter cannot be maintained for 20 years after the "armed attack" of 9/11, especially when compared to the conduct of other members of the United Nations.[9] Though international law is slowly starting to recognize the idea of accumulated events constituting an armed attack sufficient to trigger self-defence, this concept is far from settled (Bethlehem, 2012; Wilmshurst & Wood, 2013). And although the use of drones may have been lawful under the laws of armed conflict to target individuals in Al-Qaeda during the conflict in Afghanistan, this legality did not then extend to all members of Al-Qaeda everywhere in the world, nor did that protection extend once the US withdrew from Afghanistan, effectively ending the conflict in that place (Saul, 2022). There is also the prohibition against arbitrary interference with the right to life enshrined in the ICCPR (Heyns, 2013, p. 7).

[8] *Corfu Channel Case (UK v Alb)*, ICJ Rep. 1949, [29]-[35].

[9] See for example the claims of self-defence by Britain and France in 2015 in response to activities by ISIL in Syria (Delattre, 2015; Rycroft, 2015).

Perhaps unsurprisingly, US domestic law supports a contrary position. Title 50 of the US Code permits the CIA to use lethal force in counterterrorism and it is plainly apparent the CIA has used this permission extensively to undertake strikes on targets of national security interest (Wall, 2011, p. 37). Of course, US President Ronald Reagan famously banned "assassination" by Executive Order 12333 in 1981 – but the more contemporary position is that the application of lethal force as part of operations in self-defence does not and cannot constitute assassination (Bazan, 2002). US municipal and domestic courts also appear unwilling to consider the legitimacy of drone programs where they have been executed under heads of State, arguing that the question is a political and not a legal one (Jurecic, 2017).

There are lessons that can be taken from the US experience with pre-emptive strikes. This article thus suggests that a State seeking to enact a legitimate covert pre-emptive strike program require: a.) a comprehensive grounding and authorization scheme in its municipal or domestic law; b.) clear and concise legal definitions for terms such as "imminence", "threat" and "national security" in the context of the sponsoring State; c.) clear evidence of the exact assessments undertaken and advice received that left the application of lethal force as the only viable option; and d.) clear reasons for the necessity of the strike being taken as a covert action (as opposed to a military operation).

The starting point for these lessons is that US law at least comprehensively covered the field of providing authorization for pre-emptive strikes, even if the ultimate operational decisions confused whether operations were authorized under US Code Title 10 (military) or Title 50 (CIA) (Wall, 2011). That legislative basis was supported by both a declaration by Congress and executive orders under the hand of the President (Knoops, 2014, p. 44-45). There is no reason – either under international or domestic law – why these authorizations might not be rendered secret and the strikes themselves also conducted in a manner that provides for plausible deniability (Perina, 2015).

Within a legislatively authorized pre-emptive strike program, each individual strike must also comply either with the laws of armed conflict, or the legal requirements to satisfy anticipatory self-defence under Article 51 of the Charter. With respect to the first (laws of armed conflict), each individual strike must avoid civilian casualties, are directed to a specific and articulated military objective which outweighs those possible casualties, and complies with the long-standing principles of necessity, distinction and proportionality (Melzer, 2010, p. 287; Bradley & Nienaber, 2015, p. 428-429). For anticipatory self-defence to apply, there must be an "urgency" in acting on the target as well as a lack of suitable alternatives to avoid the threat to national security the State alleges.[10] This "urgency" or "imminence" is derived from the *Caroline*[11] case, and thus a situation must be clearly defined by reference to an "instant, overwhelming, and leaving no choice of means, and no moment for deliberation" (Orr, 2011, p. 740; McDonnell, 2012, p. 243).

As an alternative, in our highly digitized future there may be no need for a covert pre-emptive strike program to cause physical damage; thus, pre-emptive strikes which target infrastructure without applying kinetic force that endangers human beings may become the norm (Silver, 2002; Sanger, 2017). These strikes will be covered by the following section of this article.

[10] The bar is relatively low and may include the mining of a single seagoing vessel: *The Oil Platforms (Iran v. US) (Case)*, 2003 ICJ 189.

[11] *Caroline Incident*, 29 B.F.S.P. 1137 -1138.

Cyberattack or cyberwarfare

Cyberattacks – being the "use of information technology, such as computer network attacks or psychological operations, to influence, disrupt, corrupt, usurp, or defend information systems and the infrastructure they support" (Hollis, 2007, p. 1023) – have a very great potential to be the *de jure* of covert actors over the next century. The attraction of the typology to covert actors is perhaps because of its somewhat unique treatment under international and domestic law, which in turn derive from practical difficulties in applying physical precepts to digital concepts.

For example, does a State's use of a computer to infiltrate the information system of a neighboring or adversarial State trigger infringements of sovereignty? If an attack involves infrastructure owned by or located in the geography of a State, then sovereignty may be infringed (Schmitt & Vihul, 2017). However, what if the infrastructure of a State is being used by a second State to attack the infrastructure of a third? The answer is not clear cut and becomes a torturous working of customary international law. Margulies (2013) suggests that neither the Tallinn Manual nor the Tribunal's findings in *Tadic*[12] are fit-for-purpose in determining sovereignty issues in cyberspace, whilst Jensen (2015) suggests that the jurisprudence of international law has not sufficiently matured to provide a suitable regulatory mechanism.

That is not to say that the international law has no application in the cyber domain. For example, taking precautions in attack and removing civilians from the vicinity of objectives require relatively little amendment to apply in the context of cyberattacks (Massingham & McKenzie, 2021). Protection of civilians and civilian objects are likewise considered by the international community to be protected from cyberattack (Kilovaty, 2016, p. 127), and impose both passive and active obligations on military commanders to honour those obligations (Khawaja, 2022). The International Committee of the Red Cross (ICRC) also considers that all binding international instruments and customary international law will regulate online activity, including cyberattacks (ICRC, 2019).

At the level of domestic law, there was an early view that cyberattacks could constitute war crimes, where those countries enacted domestic legislation to ratify the Rome Statute (Graham, 1999; Silver, 2002). However, more recent developments internationally – including the 2001 Council of Europe Convention on Cybercrime (also known as the Budapest Convention) – has led to these attacks being regulated under criminal offences which outlaw unauthorized interference, destruction, tampering or theft of electronic data (Hathaway et al., 2012). Perhaps unsurprisingly, States which have enacted laws prohibiting these offences leave open the defences for those acting under "lawful government authority" such as agents of national governments, intelligence agencies and their covert actors (Hollis, 2007; Hathaway et al., 2012). The mechanisms of this "lawful government authority" differ between jurisdictions, but generally provide an exemption from prosecution for covert actors[13] or allow senior political or judicial officers to grant warrants authorizing the conduct, even where those warrants affect computers outside their host jurisdiction (Warren, Mann & Molnar, 2020).[14]

[12] Establishing that acts of individuals are attributable to a State if the State exercised "effective control" over those individuals: *Prosecutor v Tadić* (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-94-1-A, 15 July 1999).

[13] Such as countries like Australia (*Criminal Code* (Cth), ss 474.6(7) and 92.11) and Germany (*Strafgesetzbuch*, §§202a and 303a) criminalise only "unauthorized" computer offences, i.e., those conducted by an officer of the State.

[14] Both the US and UK prohibit computer offences, but render the conduct of those operating under warrants lawful (see for example *Computer Misuse Act 1990* (UK), ss 1-3ZA cf. *Intelligence Services Act 1994* (UK, s 5(1)).

 ISBN: 978-86-87043-84-8

Given the significant grey area regulating the conduct of cyberattacks, it can be hardly surprising that States have sought out these capabilities and begun using them in the "grey zone" of legal regulation. There are other motivations: the first being non-attribution (a key characteristic of covert action). The most widely published attack – involving the Stuxnet computer attack on Iranian nuclear centrifuges – was largely considered to be a joint US-Israeli covert action but was never actually formally attributed (Lindsay, 2013). The WannaCry and Petya/NotPetya ransomware attacks of 2016 and 2017 were also widely popularized as attacks by hacking groups "The Shadow Brokers" who were allegedly funded by Russia and "Lazarus", allegedly funded by North Korea. Whilst some States issued formal statements attributing the attacks to those sponsoring States, there was no public repercussions or punishment (Watney, 2019).

The second benefit of cyberattacks in a covert action setting is greater control of proportionality. Unlike a drone or missile strike, a cyberattack does not have to cause physical damage or apply kinetic force to its target. Though Stuxnet clearly caused infrastructure damage to Iran's nuclear program, there were no reported fatalities – a far cry from the predictions associated with earlier plans to conduct covert airstrikes (Lindsay, 2013, p. 379). And although the ransomware attacks of 2016 and 2017 may have caused some casualties because of lack of access to critical data in health settings, this was not its intended purpose (Watney, 2019). Cyberattacks offer a potential for covert actions to "be dialed up and dialed back… the level of damage is, theoretically, much easier to control" (Sanger, 2017, p. 71). The ability for cyberattacks to be remediated or "fixed" is also far greater. Theoretically once ransomware is "unlocked" by its key, the data remains untouched: a State could use ransomware to achieve its diplomatic or foreign policy goals, before providing the key once the targeted State accedes to its demands (Peters, 2017).

A third benefit for cyberattacks in a covert action program is the ability for the sponsoring State to create conditions allowing the action to be attributed to a third party – the perfect plausible deniability characteristic. After all, the concept of attribution for many cyberattacks is "largely a solved problem" in that the source of an attack can be forensically derived, and many States now possess advanced capabilities not just of identification, but retaliation (Alperovitch, 2018). However, there is a significant difference between attribution of individual attacks and attribution of State sponsorship of those attacks, leaving a gap which is yet to be filled either by international or domestic legal mechanisms (Rid & Buchanan, 2015; Egloff & Smeets, 2021).

Cyberattacks are not a panacea. There is evidence from empirical and case studies that without proper and robust diplomatic and foreign policy measures being undertaken in conjunction with cyberattacks, the benefits of cyberattacks are short-lived and the repercussions often disastrous (Iasiello, 2013; Gomez, 2016; Jacobsen, 2021; Sallinen, 2021). In that way, they are functionally no different to other forms of covert action, which require *overt* action to be truly successful (Radsan, 2009; Cormac, Goodman & Holman, 2016; Gomez, 2018; Cormac, & Aldrich, 2018). There are also broader concerns that the tools of developed States might, like weapons of mass destruction before them, end up in the hands of unprincipled, dangerous or criminal non-State actors with no intention of maintaining peaceful resolution of State conflicts (Sanger, 2017, p.73):

> From a keyboard in Moscow or Shanghai, Pyongyang or Tehran, the world is borderless, and information travels nearly instantaneously. No local crews are needed to maintain the weapon or refuel it. If adjustments need to be made to the weapon, the work can be done from half a world away… All cyber war can be distant, yet its effects can be local.

Conclusion

Speaking on the history of the CIA, Weiner (2007, p. 11) described the works of the agency as being a dichotomy between espionage and covert action, where "[e]spionage seeks to know the world...Covert action seeks to change the world". This article has sought to identify a place for covert action in the achievement of peace and resolution of conflict, and to describe the new typologies of covert action through the lens of legality and legitimacy.

In broad strokes, covert action will continue to be a significant tool in the foreign policy arsenal of States, potentially irrespective of whether international or domestic law outlaws individual practices. This summarises the first area of future research which this article calls for: more concise and inclusive regulatory frameworks at both international and domestic levels. Unfortunately, at the international level it is unlikely that frameworks will be enacted which either address covert action as a broad concept or the individual typologies discussed herein. Given the lack of movement towards an instrument regulating covert action in the decades during which it has been used, States appear comfortable operating without the safety net of an international legal instrument.

Therefore, States need to ensure that their domestic legal frameworks are clear and unambiguous about how, when and where (and against who) covert action may be undertaken. Intelligence agencies and their covert actors may need to obtain a warrant from a senior political, diplomatic or judicial officer, satisfying them as to the necessity and circumstances of the covert action (Caparini, 2016). Domestic legislatures may instead provide areas within which a covert agency may undertake its own actions but be subject to a form of oversight by an appropriately security cleared ombudsman or commissioner (Bochel, Defty & Kirkpatrick, 2014). These actions might still remain secret and unreleased to members of the community; however, in the event that the action is revealed or detected, there exists a strong ground for the action to be legitimized by reference to the sponsoring State's national law.

States also need to confront the emerging paradigm that covert action is an increasing part of international diplomacy and conflict resolution. The lower costs to entry for the typologies for new covert action and the benefits for those activities mean that the landscape will now be populated by more than just the two superpowers of the Cold War. Not only do States need to ensure the proper legitimacy of their covert actions abroad, but that their internal laws (and those charged with enforcing those laws) are properly equipped to confront new covert action typologies. Again, domestic laws are appropriate for the purpose and should "expand the reach of domestic law abroad and develop a system for utilizing limited countermeasures" to covert actions (Hathaway et al., 2012, p. 885).

Of course, these actions will be fragmented and patchwork as they are enacted by individual States, influenced by all the traditional impacts on their domestic judicatures. What will eventually be needed in some uncomfortable conversations in the international community about what is deemed acceptable in the shadowed world of covert action. States will need to be candid in this at least and take the conversation beyond "we and our friends merely gather information; you and your type violate sovereignty" (Pun, 2017, p. 355). Whilst an international treaty that regulates espionage, spying and covert action is unlikely to be realized, the absence of *anything* is unlikely to constrain or discourage States in seeking every tool to pursue this third way of diplomacy.

Acknowledgments

I would like to thank the T.C. Beirne School of Law at The University of Queensland for providing the funding for travel to attend the PCRC 2022.

Funding

This research received no external funding.

Conflict of interest

Author declares no conflict of interest.

References

Aldrich, R. J., Cormac, R. (2016). *The Black Door: Spies, Secret Intelligence and British Prime Ministers*. London: William Collins.

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research, 58*(5), 1083-1097.

Alperovitch, D. (2018, January 28). Stopping the Next Cyber Conflict. *The Cipher Brief.* https://www.thecipherbrief.com/column_article/stopping-next-cyber-conflict

Andrew, C. (1995). *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. London: HarperCollins.

Andrew, C. (2004). Intelligence, international relations and "under-theorisation". *Intelligence and National Security, 19*(2), 170-184.

Banka, A. (2014). *US Targeted Killing, Secrecy and the Erosion of the Assassination Norm* [PhD thesis, University of Birmingham]. University of Birmingham Research Repository. https://etheses.bham.ac.uk/id/eprint/7443/1/Banka17PhD.pdf

Banks, W. (2017). State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. *Texas Law Review*, *95*(7), 1487-1514.

Baxter, R. (2013). So-Called "Unprivileged Belligerency": Spies, Guerrillas, and Saboteurs. In D. F. Vagts, T. Meron, S. M. Schwebel, C. Keever (Eds.), *Humanizing the Laws of War: Selected Writings of Richard Baxter*, pp. 37-44.

Bazan, E. (2002). *Assassination Ban and E.O. 12333: A Brief Summary*. CRS Report for Congress. https://digital.library.unt.edu/ark:/67531/metacrs2392/

Beard, J. M. (2014). Legal phantoms in cyberspace: The problematic status of information as a weapon and a target under international humanitarian law. *Vanderbilt Journal of Transnational Law, 47*(1), 67-144.

Bethlehem, D. (2012). Self-defense against an imminent or actual armed attack by nonstate actors. *American Journal of International Law, 106*(4), 770-777.

Bochel, H., Defty, A., & Kirkpatrick, J. (2014). *Watching the Watchers: Parliament and the Intelligence Services*. Dordrecth: Springer.

Boister, N. (2018, September). Global simplification of extradition: interviews with selected extradition experts in New Zealand, Canada, the US and EU. *Criminal Law Forum, 29*(3), 327-375.

Bradley, M., & Nienaber, A. (2015). The Use of Drones for Cross-Border Law Enforcement and Military Purposes in Another State's Sovereign Airspace: A Legal Analysis. *Hungarian Yearbook of International Law and European Law*, 411-432.

Brown, J. N. 2014. The Sound of Silence: Power, Secrecy, and International Audiences in US Military Basing Negotiations. *Conflict Management and Peace Science, 31*(4), 406-431.

Caparini, M. (2016). Controlling and overseeing intelligence services in democratic states. In M. Caparini, H. Born (Eds.), *Democratic Control of Intelligence Services* (pp. 3-24). Routledge.

Carnegie, A., Kertzer, J. D., Yarhi-Milo, K. (2022). Democratic Peace and Covert Military Force: An Experimental Test. *Journal of Conflict Resolution*, DOI: 10.1177/00220027221116289, 1-31.

Carson, A. 2016. Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War. *International Organization, 70*(1): 103–31.

Coe, B. (2015). Sovereignty regimes and the norm of noninterference in the global south: regional and temporal variation. *Global Governance, 21*(2), 275-298.

Cooke, P. (2010). Bringing the Spies in from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War. *University of San Francisco Law Review, 44*(3), 601-658.

Cormac, R., Goodman, M. S., & Holman, T. (2016). A Modern-Day Requirement for Co-Ordinated Covert Action. *The RUSI Journal, 161*(2), 14-21.

Cormac, R., Aldrich, R. J. (2018). Grey is the new black: covert action and implausible deniability. *International Affairs, 94*(3), 477-494.

Cormac, R., Walton, C., van Puyvelde, D. (2022). What constitutes successful covert action? Evaluating unacknowledged interventionism in foreign affairs. *Review of International Studies, 48*(1), 111-128.

Couzigou, I. (2021). The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression. *Election Law Journal: Rules, Politics, and Policy, 20*(1), 98-115.

Damrosch, L. F. (1989). Politics across borders: Nonintervention and nonforcible influence over domestic affairs. *American Journal of International Law, 83*(1), 1-50.

Delattre, F. (2015). Identical letters dated 8 September 2015 from the Permanent Representative of France to the United Nations addressed to the Secretary-General and the President of the Security Council. UN Doc S/2015/745.

Downes, A. B., Lilley, M. L. (2010). Overt Peace, Covert War?: Covert Intervention and the Democratic Peace. *Security Studies, 19*(2), 266-306.

Egloff, F. J., Smeets, M. (2021): Publicly attributing cyber attacks: a framework, *Journal of Strategic Studies*, DOI: 10.1080/01402390.2021.1895117.

Enterline, A. J., Greig, M. (2008). Perfect Storms? Political Instability in Imposed Polities and the Futures of Iraq and Afghanistan. *Journal of Conflict Resolution, 52*(1), 880-915.

Evans, R. 2014. Machiavelli's 27 Rules of War. *War on the Rocks*. https://warontherocks.com/2014/08/machiavellis-27-rules-of-war/

Fabre, C. (2022). *Spying Through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence*. Oxford University Press: Oxford.

Forsgren, B. (2021). Death Star Drones: How Missile Defense Drone Technology Marks the Advent of Contingent Sovereignty. *Brigham Young University Law Review, 46*, 847-882.

Frolov, S. (2007). The Semiotics of Covert Action in 1 Samuel 9—10. *Journal for the Study of the Old Testament, 31*(4), 429-450.

Fuller, C. J. (2017). *See It/Shoot It: The Secret History of the CIA's Lethal Drone Program*. Yale University Press.

Gentry, J. A. (2016). Toward a Theory of Non-State Actors' Intelligence. *Intelligence and National Security, 31*(4), 465-489.

Giles, L. (2005). *Translation of Sun Tzu's The Art of War* (Tuttle Classics: London).

Gomez, M. A. N. (2016). Arming cyberspace: The militarization of a virtual domain. *Global Security & Intelligence Studies, 1*(2), 27786.

Gomez, M. (2018). When less is more: Cognition and the outcome of cyber coercion. *Cyber, Intelligence, and Security, 2*(1), 3-19.

Graham, B. (1999, November 8) Military Grappling with Guidelines for Cyberwar. *Washington Post*. https://www.washingtonpost.com/wp-srv/national/nat001.htm

Haciyakupoglu, G., Hui, J. Y., Suguna, V. S., Leong, D., & Rahman, M. F. B. A. (2018). *Countering fake news: A survey of recent global initiatives*. Nanyang Technological University: Rajaratnam School of International Studies.

Hamilton, L. (2017). Beyond Ballot-Stuffing: Current Gaps in International Law Regarding Foreign State Hacking to Influence a Foreign Election. *Wisconsin International Law Journal*, *35*(1), 179-204.

Hansen, I., & Lim, D. J. (2019). Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics, 25*(2), 150-171.

Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817-886.

Henderson, S. C. (2019). *Policy, Politics and the Public: The securitization of foreign interference in North America*. Research paper. University of Ottawa: Graduate School of Public and International Affairs.

Her Majesty's Government. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948). London: The Stationery Office.

Heyns, C. (2013). *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*. UN Doc A/68/382.

Hollis, D. B. (2007). Why states need an international law for information operations. *Lewis & Clark Law Review, 11*(4), 1023-1062.

Iasiello, E. (2013, June). Cyber attack: A dull tool to shape foreign policy. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1-18. IEEE.

International Committee of the Red Cross (ICRC). (2019). *International Humanitarian Law and Cyber Operations during Armed Conflicts*. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

Jacobsen, J. T. (2021). Cyber offense in NATO: challenges and opportunities. *International Affairs, 97*(3), 703-720.

James, P, Mitchell, G. E. (1995). Targets of Covert Pressure: The Hidden Victims of the Democratic Peace. *International Interactions, 21*(1), 85-107.

Jensen, B., Valeriano, B., Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies, 42*(2), 212-234.

Jensen, E. T. (2015). Cyber sovereignty: The way ahead. *Texas International Law Journal, 50*(2-3), 275-304.

Johns, R., Davies, G. A. M. (2012). Democratic Peace or Clash of Civilizations? Target States and Support for War in Britain and the United States. *The Journal of Politics, 74*(4), 1038-1052.

Johnson, L. K. (1989). Covert Action and Accountability: Decision-Making for America's Secret Foreign Policy. *International Studies Quarterly, 33*(1), 81-109.

Johnson, L. K. (2020). Reflections on the ethics and effectiveness of America's 'third option': covert action and U.S. foreign policy. *Intelligence and National Security, 35*(5), 669-685.

Johnson, L. K. (2021). Ethics and covert action: The "Third Option" in American foreign policy. In S. Miller, M. Regan, & P. F. Walsh (Eds.), *National Security Intelligence and Ethics* (pp. 169-186). Abingdon: Routledge.

Joseph, M. F., Poznansky, M. (2018). Media Technology, Covert Action, and the Politics of Exposure. *Journal of Peace Research, 55*(3), 320-335.

Jurecic, Q. (2017, June 30). US Court of Appeals for the DC Circuit Dismisses Suit Over US Drone Strike. *Lawfare*. https://www.lawfareblog.com/us-court-appeals-dc-circuit-dismisses-suit-over-us-drone-strike

Kalugin, O. (1994). *The First Directorate: My 32 Years in Intelligence and Espionage against the West.* Smith Gryphon: London.

Kasher, A., Yadlin, A. (2005). Assassination and Preventive Killing. *SAIS Review of International Affairs, 25*(1), 41-57.

Keohane, R. O. (1997). International Relations and International Law: Two Optics. *Harvard International Law Journal, 38*(2), 487-502.

Khawaja, A. A. (2022, August 17). *Cyber Warfare and International Humanitarian Law*. DLP Forum. https://www.dlpforum.org/2022/08/17/cyber-warfare-and-international-humanitarian-law/.

Kibbe, J. D. (2022). CIA/SOF convergence and congressional oversight. *Intelligence and National Security*, 1-17. https://doi.org/10.1080/02684527.2022.2104015

Kilovaty, I. (2016). Virtual Violence - Disruptive Cyberspace Operations as Attacks under International Humanitarian Law. *Michigan Telecommunications and Technology Law Review 23*(1), 113-127.

Kim, J. (2005). Democratic Peace and Covert War: A Case Study of the US Covert War in Chile. *Journal of International and Area Studies, 12*(1), 25-47.

Knoops, G. (2014). Drones at trial: state and individual (criminal) liabilities for drone attacks. *International Criminal Law Review, 14*(1), 42-81.

Lahmann, H. (2020). Information Operations and the Question of Illegitimate Interference Under International Law. *Israel Law Review, 53*(2), 189-224.

Levin, D. H. (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results. *International Studies Quarterly, 60*(2), 189-202.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404.

Madden, D., Hoffmann, D., Johnson, M., Krawchuk, F. T., Nardulli, B. R., Peters, J. E., Robinson, L., Doll, A. (2016). *Toward operational art in special warfare*. Rand Corporation: Santa Monica.

Margulies, P. (2013). Sovereignty and cyber attacks: Technology's challenge to the law of state responsibility. *Melbourne Journal of International Law, 14*(2), 496-519.

Massingham, E., McKenzie, S. (2021). Taking Care Against the Computer. *Journal of International Humanitarian Legal Studies, 12*(2), 224-250.

McDonnell, T. M. (2012). Sow What You Reap? Using Predator or Reaper Drones to Carry Out Assassinations or Targeted Killings of Suspected Islamic Terrorists. *George Washington International Law Review 44*(2), 243-316.

McNeal, G. (2009). National security symposium: the battle between Congress & the courts in the face of an unprecedented global threat. *Regent University Law Review, 21*(2), 331-347.

Melzer, N. (2010). Targeted killings in operational law perspective. In T. D. Gill & D. Fleck (Eds.), *The Handbook of the International Law of Military Operations*. Oxford: Oxford University Press, 277-302.

Mohan, V., Wall, A. (2019). Foreign Electoral Interference: Past, Present and Future. *Georgetown Journal of International Affairs 20*(1), 110-118.

Ohlin, J. (2017). Did Russian cyber interference in the 2016 election violate international law. *Texas Law Review, 95*(7), 1579-1598.

Omand, D., and Pythian, M. (2021). The technoethics of contemporary intelligence practice: A framework for analysis. In S. Miller, M. Regan, & P. F. Walsh (Eds.), *National Security Intelligence and Ethics* (pp. 39-60). Abingdon: Routledge.

O'Rourke, L. A. (2018). *Covert Regime Change: America's Secret Cold War*. Cornell University Press: Cornell.

O'Rourke, L. A. (2020). The Strategic Logic of Covert Regime Change: US-Backed Regime Change Campaigns during the Cold War. *Security Studies, 29*(1), 92-127.

Orr, A. C. (2011). Unmanned, unprecedented, and unresolved: the status of American drone strikes in Pakistan under international law. *Cornell International Law Journal, 44*(3), 729-752.

Peic, G., & Reiter, D. (2011). Foreign-imposed regime change, state power and civil war onset, 1920-2004. *British Journal of Political Science, 41*(3), 453-475.

Perina, A. H. (2015). Black Holes and Open Secrets: The Impact of Covert Action on International Law. *Columbia Journal of Transnational Law, 53*(3), 507-583.

Perley, S. (2016). *Arcana imperii: Roman political intelligence, counterintelligence, and covert action in the Mid-Republic* (Doctoral dissertation, The Australian National University (Australia)).

Peters, M. (2017). Cyber Enhanced Sanction Strategies: Do Options Exist? *Journal of Law and Cyber Warfare, 6*(1), 95-154.

Poznansky, M. 2015. Stasis or Decay? Reconciling Covert War and the Democratic Peace. *International Studies Quarterly, 59*(4): 815-826.

Pun, D. (2017). Rethinking espionage in the modern era. *Chicago Journal of International Law*, *18*(1), 353-391.

Radsan, A. (2009). An overt turn on covert action. *Saint Louis University Law Journal, 53*(2), 485-552.

Regan, M. (2022, June 2). Drone Strikes and Evidence-Based Counterterrorism. *Lawfare*. https://www.lawfareblog.com/drone-strikes-and-evidence-based-counterterrorism

Regan, M., & Poole, M. (2021). Accountability for covert action in the United States and the United Kingdom. In S. Miller, M. Regan, & P. F. Walsh (Eds.), *National Security Intelligence and Ethics* (pp. 232-248). Abingdon: Routledge.

Rid. T., Buchanan, B. (2015). Attributing Cyber Attacks. *The Journal of Strategic Studies, 38*(1–2), 4-37.

Ross, T. (2022). The Weight of a Word: 'Covert' and the Proportionality of Australia's Foreign Interference Laws. *Federal Law Review,* 1-31, DOI: 10.1177/0067205X221107409.

Rycroft, M. (2015). Letter dated 7 September 2015 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council. UN Doc S/2015/688.

Sallinen, M. (2021). *Weaponized malware, physical damage, zero casualties–what informal norms are emerging in targeted state sponsored cyber-attacks?: The dynamics beyond causation: an interpretivist-constructivist analysis of the US media discourse regarding offensive cyber operations and cyber weapons between 2010 and 2020* [PhD thesis, Swedish Defence University]. Research Repository. https://www.diva-portal.org/smash/get/diva2:1527278/FULLTEXT01.pdf

Sanger, D. E. (2017). Cyber, Drones, and Secrecy. In G. Perkovich & A. E. Levite (Eds.), *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown: Georgetown University Press.

Sanders, R. (2011). (Im)plausible legality: the rationalisation of human rights abuses in the American 'Global War on Terror'. *The International Journal of Human Rights, 15*(4), 605-626.

Saul, B. (2022, August 17). The Unlawful U.S. Killing of Ayman al-Zawahri. *Lawfare*. https://www.lawfareblog.com/unlawful-us-killing-ayman-al-zawahri

Schmitt, C. (2005). *Political Theology: Four Chapters on the Concept of Sovereignty*. Chicago: University of Chicago Press.

Schmitt, M. N. (2018). "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law. *Chicago Journal of International Law*, *19*(1), 30-67.

Schmitt, M. N., Vihul, L. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Sheldon, R. M. (1997). The ancient imperative: clandestine operations and covert action. *International Journal of Intelligence and Counterintelligence*, *10*(3), 299-315.

Silver, D. B. (2002). Computer network attack as a use of force under Article 2(4) of the United Nations Charter. *International Law Studies, 76*(1), 21-97.

Smith, W. C. (2004, 14 July). Sabotage: Its History, Philosophy & Function (website, International Workers of the World) <https://archive.iww.org/history/library/WCSmith/sabotage/>.

Starbird, K., Arif, A., Wilson, T. (2019). Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1-26. https://doi.org/10.1145/3359229.

Stempel, J. D. 2007. Covert Action and Diplomacy. *International Journal of Intelligence and Counterintelligence, 20*(1), 122-135.

Stoltz, W. A. (2022). *A Regrettable Necessity: The Future of Australian Covert Action*. Canberra, National Security College. https://nsc.crawford.anu.edu.au/publication/20309/regrettable-necessity-future-australian-covert-action

Tomz, M. R., & Weeks, J. L. (2013). Public opinion and the democratic peace. *American political science review, 107*(4), 849-865.

Urban, M. (1992). *Big Boys' Rules: The SAS and the Secret Struggle against the IRA.* Faber & Faber: London.

US. Congress.gov. (2022). *S.1325 - Intelligence Authorization Act, Fiscal Year 1991.* https://www.congress.gov/bill/102nd-congress/senate-bill/1325

Wall, A. E. (2011). Demystifying the title 10-title 50 debate: Distinguishing military operations, intelligence activities & covert action. *Harvard National Security Journal, 3*(1), 85-142.

Warner, M. (2019). A matter of trust: Covert action reconsidered. *Studies in Intelligence, 63*(4), 33-41.

Warren, I., Mann, M., & Molnar, A. (2020). Lawful illegality: Authorizing extraterritorial police surveillance. *Surveillance & Society, 18*(3), 357-369.

Watney, M. (2019). A Legal Understanding of State-Linked Cyberattacks and Malicious Cyber Activities. *European Conference on Cyber Warfare and Security*. Reading: Academic Conferences International Limited.

Weiner, T. (2007). *Legacy of Ashes: The History of the CIA*. New York: Doubleday Books.

Wilmshurst, E., & Wood, M. (2013). Self-Defense Against Nonstate Actors: Reflections on the "Bethlehem Principles". *American Journal of International Law, 107*(2), 390-395.

Wittes, B. (2014, June 24). Whence Imminence in that Drone Memo? A Puzzle and a Theory. *Lawfare*. https://www.lawfareblog.com/whence-imminence-drone-memo-puzzle-and-theory

Wittmer, L. A. (2013). *Covert coercion: a formal analysis of unconventional warfare as an interstate coercive policy option.* Monterey, California: Naval Postgraduate School.

Zegart, A. B. (2022). *Spies, Lies, and Algorithms: The History and Future of American Intelligence.* Princeton University Press: Oxford.