A Matter of Trust: Covert Action Reconsidered

Michael Warner

Covert action is the secret supplement to war and diplomacy, employed at the margins of conflict to shift patterns of trust and allegiance.

Increasing our knowledge of what covert action is requires deeper insight into how it works, especially in the cyber domain. Covert action is the secret supplement to war and diplomacy, employed at the margins of conflict to shift patterns of trust and allegiance. With most if not all types of covert actions, however, the problem has always been one of scale. Covert action to be effective has had to remain plausibly deniable for a crucial time period, and to do so it has had to remain small. Cyberspace with its promises of (relative) anonymity and its near-instantaneous reach to large numbers of computer users has made it possible to run activities that are indistinguishable from covert actions on a much larger scale. That development does not make all cyberspace operations covert actions; rather, it suggests that cyber covert actions will be practiced by many more nations unless and until victim states find ways of thwarting them.

Covert action's dark arts have been with us at least as long as we have written records, but they have always been marginal to the larger movements of politics, diplomacy, and war. This limitation inheres in the secrecy that by definition attends *covert* action. After all, something is covert if its effects can be seen but something about its origin, sponsorship, or purpose remains deliberately hidden from those who would certainly want to know the full truth about it.

Such secrecy is naturally difficult to maintain, and embarrassing or even fatal to lose. Hence covert action's influence on the margins of state practice in war, diplomacy, and internal security. As soon as it scales up to a point where its secret aspects can no longer be kept secret, then it either fails or finds itself subsumed within larger, overt activities or operations. That rule may now be changing as a result of the ease with which states and non-state actors can mount covert (i.e., unattributed) campaigns in and through cyberspace.

Ancient Roots, Modern Scholarship

Ancient authors had plenty to say about spies, and though they regaled readers with examples of political and military skulduggery, they typically glossed over the distinctions between practices that we moderns would carefully distinguish, such as espionage (the clandestine collection of secrets) and covert action (the various arts of subversion and sabotage). A spy was a spy; for purposes of taxonomy it mattered little whether he collected secrets in the enemies'

The views, opinions, and findings of the author expressed in this article should not be construed as asserting or implying US government endorsement of its factual statements and interpretations or representing the official positions of any component of the United States government.

Classical authors who were quite distant from one another in time, place, and culture nonetheless sound remarkably similar when addressing indirect and subtle means to cause effects.

camp or poisoned their general.[a] What counted most for authors like Sun Tzu, Kautilya, and Plutarch was not the morality of treason and trickery, or the taxonomy of the spy's actions, but the fact that the spy had gained trusted access to the enemy's plans and person. Such entrée was highly useful to, and thus prized by, the spy's secret master, who could exploit it for a variety of ends.

Classical authors who were quite distant from one another in time, place, and culture nonetheless sound remarkably similar when addressing indirect and subtle means to cause effects. Such means were not exactly what we now call covert action, but were well known and, if not approved, then were at least an expected supplement to war and diplomacy, used when normal practices did not avail. The late Adda Bozeman reminded scholars that the primary actor in covert actions is not the state per se but the regime running that state; not a few regimes, she noted, have practiced covert action against their domestic rivals rather than (or in addition to) their foreign opponents.[1]

Though ancient, covert action as such has been defined and studied only for a few decades now. The need to safeguard international legitimacy was a factor in the frequency of "secret wars" during the ensuing Cold War. Austin Carson has usefully examined several cases of covert interventions (specifically in Korea, Vietnam, and Afghanistan), in which external powers provided lethal aid to combatants, or even fought each other, while ostensibly hiding their roles in wars that were already ongoing. Carson notes that both sides, however, knew full well of this covert assistance and even combat, and yet decided not to publicize it.

The resulting "collusion" between rival states to maintain the obscurity of certain aspects of larger conflicts served an important, rational purpose for both sides: it preserved bargaining space by mitigating "hawkish" internal pressures in one side or both that could have escalated the conflicts.[2] This notion of limiting escalation and preserving bargaining space is an important argument that Carson makes, and one could easily add to it another incentive for secrecy: the desire to preserve the diplomatic legitimacy essential for international coalition building. In short, given modern strictures on aggressive war, a state gains more allies for its preferred policies and allies if its behavior is viewed as following international law and norms—and if the behavior of its opponents is seen as violating them.

Legislative and scholarly considerations of covert action ultimately led in the United States to passage of a law to define and govern it. This was arguably the first statute in history to openly define the practice; before this point covert action had just been something that states did even if they did not talk about it. The (then) annual Intelligence Authorization Act for Fiscal Year 1991 defined covert action as "an activity or activities conducted by, or on behalf and under the control of, an element of the US government to influence political, economic, or military conditions abroad so that the role of the United States is not intended to be apparent or acknowledged publicly."[3] That is, covert action means methods designed to influence foreign events in ways that will not convincingly be attributed to the US government. That "plausible deniability" of visible effects subsequently seems to have become a universal definition.

The definition fixed by the US Congress is a good one not only because of what it includes but for what it leaves out. First, it implicitly distinguishes *covert* activities (which are visible by definition, while their sponsorship remains hidden) from *clandestine* ones (both the cause *and* the effect of which are intended to remain invisible). Second, the definition does not encompass normal diplomatic practices or military tactics, even military deception measures. The former are typically conducted between declared diplomats in agreed and publicly known settings, such as ministries and embassies. The latter are similarly conducted by one's own forces and often in full view of the adversary, and thus they are hardly unattributable, even if their import is not what it seems. Congress deemed such "traditional diplomatic or military activities" to remain outside

[a] "Generally, in the case of armies you wish to strike, cities you wish to attack, and people you wish to assassinate, you must first know the names of the garrison commander, the staff officers, the ushers, gate keepers, and the bodyguards. You must instruct your agents in inquire into these matters in minute detail." Sun Tzu, *The Art of War*, Samuel B. Griffith trans. (London: Oxford, 1963), chapter 13.

the ambit of covert action and thus beyond the reach of statutes governing it.[4]

A word about the scholarship on covert action seems appropriate before we move on. Covert action as defined above implied certain affinities between covert action and diplomacy. To wit, covert action does not always impact "targets"; sometimes it seeks partners (who can in turn work together against the same targets). Len Scott noticed this in 2004, when he usefully described "clandestine diplomacy." Scott's term denoted "secret and deniable discussions with adversaries," specifically "an activity undertaken by secret intelligence services where deniable communications between adversaries may be helpful."[5]

One might well ask what countries (and terrorist groups) locked in a de facto or even a de jure state of armed conflict would have to say. It turns out that they sometimes have plenty to talk about, as Scott hints and history verifies. Wartime parleys under a flag of truce have a long pedigree, of course, but that is not quite what Scott meant. Rather, the historical record shows any number of instances where wars and undeclared conflicts end as a result of secret negotiations that statesmen sprang upon their respective nations just before the shooting stopped. The list of crises defused by such secret talks before the shooting even started must be even longer.

Such clandestine diplomacy must proceed in secrecy, as Scott explains, because a leak could ruin the slim chance of some sort of progress toward bringing their dispute to a conclusion. Traditional diplomacy takes place between people who are publicly authorized and indeed expected to talk with one another—i.e., diplomats and high state officials. They might keep their proceedings confidential, of course, but no one disputes the seemliness of their meetings. Clandestine diplomacy, on the other hand, occurs between officials on both sides who are officially *not* supposed to talk to one another, and who keep the secret of their contacts from many (if never all) of their colleagues, countrymen, and allies. They represent states, movements, alliances that are officially in conflict, and their colleagues and coalition members might well be opposed (perhaps violently so) to the very idea of talking to the enemy.

Clandestine diplomacy, on the other hand, occurs between officials on both sides who are officially not supposed to talk to one another, and who keep the secret of their contacts from many (if never all) of their colleagues, countrymen, and allies.

Hence the secrecy of not only the proceedings but the meetings themselves, and hence the frequent involvement of intelligence officers or means in such cases. Both covert action and clandestine diplomacy can occur in conjunction, with each complementing the other. The symmetry between covert action and clandestine diplomacy allows us, for the sake of discussion in the analysis that follows, to fold in clandestine diplomacy as another type of covert action and use the latter term to denote both (unless they are explicitly distinguished). Now for some summary conclusions before considering recent trends.

Covert Action's Principles: Trust and Scale

These findings permit us to venture into theory in order to link covert action to larger understandings of political coercion, international relations, and expected utility. As noted at the outset, covert action generically is the *secret* supplement to war and diplomacy. It is not an independent factor in international relations, as Kristian Gustafson explains, for "covert action is encompassed by the same political philosophical factors which condition any non-consensual activity."[6]

Aaron Brantly helpfully explains that covert action abides in the "shadows of international relations" because it is rational in the sense that war can be rational; it is predicated on expected net utility to increase the bargaining space for two international actors who would otherwise have to fight (or keep fighting) to resolve their differences.[7] Such shadowy means are attempted when the traditional means of war and diplomacy lack efficacy, as in a situation that is not quite peace or war but perhaps has reached a tipping point between these opposites. Thus covert action is *marginal*, in the economic sense of the term, offering rulers an extra bit of diplomatic or military utility in exchange for incrementally small (but potentially consequential) "inputs" of a state's resources added to solve a problem via indirect means.

To be effective, covert action should remain plausibly deniable for a crucial time period, making it akin to wartime operational secrecy for military planners and commanders.

The Workings of CA

Having noted what covert action is, we can explore how covert action works. That marginality of covert action in turn suggests three generalizations.

First, to be effective, covert action should remain plausibly deniable for a crucial time period, making it akin to wartime operational secrecy for military planners and commanders. Like them, the architects of a covert action are typically seeking specific effects and mission outcomes, and thus certain secrets about their activities need remain secret only until a mission is accomplished. Covert action therefore has a high requirement for secrecy up to the point of mission accomplishment, after which the requirement lessens (and sometimes vanishes altogether). That is why the US government, for instance, felt able to acknowledge the "fact of" (but not the details of) some of its covert actions from World War II and the Cold War.[a]

The second generalization follows from the first: covert action is about trust. It is employed at the margins of conflict, as noted above, to split foes from each other, or to shift neutrals into one's own camp. To put this another way, covert action seeks, through secret ways, to make foes distrust one another, or make neutrals distrust foes. But sophisticated covert action (especially its clandestine diplomacy annex) does something more constructive as well: it seeks to offer less-hostile foes and/or neutrals a path away from one's harsher and more dedicated enemies. It splits the opponent's camp, and adds to one's own. Sun Tzu glimpsed this when he ranked the various policies to employ in defeating the enemy:

> *Thus, what is of supreme importance in war is to attack the enemy's strategy. Next best is to disrupt his alliances. The next best is to attack his army. The worst policy is to attack cities. Attack cities only when there is no alternative.*[8]

Covert action corresponds to Sun Tzu's second best policy: the disruption of the enemy's alliances. The successful ruler or commander induces his opponent's external allies to sit out the conflict, and his foe's internal sources of support to desert his cause. Kristian Gustafson noticed this in a recent paper: "Since no political entity above the individual is monolithic, covert action seeks to exploit whatever degree of agreement can be found within aspects of the opposing party—exploiting fine political fissures to break down an enemy's alliance."[9] If conventional military operations and tactics can be compared to the movement of pieces on a chessboard, covert action then equates to a quiet struggle to determine the shape of that board and the number of pieces each player controls.

Covert action on its own is only the catalyst for that rupture in the enemy's alliance or internal cohesion. The actual split must be facilitated; it requires a path that is provided by diplomacy, whether quiet or overt, and possibly also supplemented by military assistance or support. Here is where clandestine diplomacy fits in. It is the flip side to covert action, in that it seeks in secret to build trust with certain foes (those who want to leave the fight, or switch sides), while covert action seeks to erode or even break that trust.

Third and finally, with all of the ways and means discussed above, the problem has always been one of scale. Covert action to remain covert has to be small. It only becomes large (and known) at the point of decision. Two examples from the Second World War illustrate the point. The United States and Britain in 1943 jointly proclaimed a policy of unconditional surrender to the Axis, meaning Washington and London would not negotiate any armistice; peace would only come with utter capitulation by the Germans, Italians, and Japanese.

Yet, negotiate American and British officials certainly did in at least two instances: when the king of Italy and his government pulled Italy out of the Axis in September 1943, and when the German forces in northern Italy laid down their arms a week before VE Day. Both negotiations

[a] OSS publicized clandestine diplomacy in North Africa and Thailand, for instance, within months of the end of the war. Director of Central Intelligence Robert Gates publicly acknowledged several covert actions weeks after the collapse of the Soviet Union; see his "CIA and Openness" speech to the Oklahoma Press Association, February 21, 1992; accessed January 19, 2019 at https://fas.org/irp/eprint/gates1992.html

took place between individuals and small teams of military officers deputized by their commanders for the purpose.[10] But while both deals could be cut in secret, the execution had to become public and had to involve hundreds, if not thousands, of Allied commanders, officials, diplomats and ultimately troops.

When covert action is not small, it isn't secret, which typically means it is blown, soon or already embarrassing its sponsors and its participants. Covert action operations are usually too small to make a difference if they become publicly exposed. When they are blown their authors get the worst of both worlds: failure and notoriety. This fits with the perhaps coincidental confluence between the observations of Len Scott and Austin Carson, who both noticed that rival states in a conflict might seek through secret means to signal each other that a turning point in the struggle could be approaching (one that can either lead to escalation or de-escalation). Obviously such states have ample means of signaling one another through overt channels; diplomacy, military moves, and propaganda represent the usual mechanisms. But how can a state subtly signal that its declared policies *might* be about to change? The subtlety here is key, for it almost by definition requires quiet, plausibly deniable, and potentially reversible measures. In short, it is tailor-made for covert action.

Covert Action and Cyberspace

These factors function in new and still indeterminate ways in cyberspace, the newest "domain" of conflict. Herein lies a tale, for the relation of covert action to state activities in cyberspace has recently garnered scholarly attention. Cyberspace has its own ways and means by which opponents use force against one another, which means military force works differently, and diplomacy can operate in novel ways as well. Much of the difference in cyberspace stems from the ease of anonymity; the ability of actors to move undetected, unnoticed, or unattributed in cyberspace has become so familiar as to be verging on proverbial.

Cyberspace has its own ways and means by which opponents use force against one another. . . .

Several scholars have argued that covert action functions in cyberspace. Aaron Brantly explained in 2016 that offensive cyberspace actions are akin to covert actions because both proceed in some degree of secrecy; both sorts of operations "need to occur in the shadows between overt diplomacy and war."[11] William Carruthers in his thoughtful Ph.D. dissertation goes even further, arguing that offensive cyberspace operations are not a *form* of covert action but instead should be treated as covert action *per se.*[12]

Some evidence seems to bear this out. Brantly reflected that conceiving of offensive cyberspace operations as a simply overt tool would "overlook most state uses of cyber" since 2000.[13] Indeed, Benjamin Jensen and Brandon Valeriano argue that most of the cyberspace operations that they could count in effect constituted covert actions:

> *Despite increasingly sophisticated operations, between 2000 and 2016 cyberspace was a domain defined by political warfare and covert signaling to control escalation more than it was an arena of decisive action.*[14]

Jon Lindsay and Erik Gartzke offer a rationale to explain that pattern: "By and large, cyber options fill out the lower end of the conflict spectrum, when deterrence is not as credible or reliable." The exceptions to this rule that Lindsay and Gartzke observe are "mainly powerful states conducting covert action, subversive propaganda, or battlefield support operations against militarily weaker opponents."[15]

If the cyber domain thus seems tailor-made for covert action, there remains uncertainty over what that means. Few should be surprised that the US Congress does not closely follow debates in international relations theory, but Congress recently passed legislation moving this topic in a different direction. To wit, in August 2018 the new National Defense Authorization Act (for Fiscal Year 2019) amended Title 10 of the US Code to affirm that clandestine US military operations against adversary activities in cyberspace do not have to be regulated and overseen like covert actions: such an activity or operation by American forces could instead be treated as "traditional military activity" under the exceptions provided for in the covert action statute discussed earlier.

Why this divide between theory and practice? Here is where recent events want explication in light of the above. Over the last decade we have seen states and non-state actors (particularly terrorist groups) employ ways to attack digital information systems and the data on them. Armed forces have created cyber units to defend national networks and in recent years have used them on the offense.

The Russian effort to affect the 2016 US election campaign showed the possibilities for covert action at-scale.

But cyber conflict has spread well beyond war zones; indeed, various actors have found ways to impose their wills by non-violent means on state and non-state victims. In short, states are now employing cyber campaigns in pursuit of strategic advantage in competition short of armed conflict with one another and with non-state entities as well.

Cyberspace allows states to conduct operations that look much like covert action just as cheaply but far more broadly. Here it bears noting that the rest of the world has not imitated our legal segregation of traditional military activities (Title 10) from covert action operations (Title 50). In short, adversary states undertake secret activities without worrying whether American lawyers would classify an analogous American operation as proceeding under Title 10 or Title 50 authorities. Cyberspace further blurs the distinction. Its offers (relative) anonymity, and its near instantaneous delivery of finely tailored appeals to thousands or even millions of computer users provides the venue and means to do what covert actions once could attempt at a fraction of the extent. Indeed, cyberspace seems to have fixed covert action's problem of scale. Yes, states have been "caught" aiding and abetting such operations, as the examples below will show, but attribution is not proof, and sometimes attribution may actually appeal to certain actors.

The Russian effort to affect the 2016 US election campaign showed the possibilities for covert action at-scale. Special Counsel Robert Mueller's investigation probed the interference undertaken by the private Russian organization called the Internet Research Agency (IRA) that had close ties to Putin's regime. The Mueller Report subsequently concluded:

> *By the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants. IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple U.S. political figures who retweeted IRA-created content.*[16]

The scope of cyber-enabled efforts like the IRA's quite simply dwarfs anything possible before the Internet. Even radio broadcasts to entire countries during the Cold War did not make active, unwitting participants of their audiences; passive listening and even discussing last night's news lacks the authenticity and immediacy of a re-Tweet that perfectly replicates and spreads covert action messages produced by a foreign power.

We cannot know how many or even if any votes were swayed in 2016, but rigging the election was apparently not the operation's purpose. Its goal becomes clear in the affidavits released in early 2018 by Mueller's investigation. According to the indictment of 13 Russians handed up by his team that February, for instance, Moscow soon after its seizure of Crimea had mounted a covert campaign to get Americans arguing with one another. The IRA "as early as 2014 . . . began operations to interfere with the U.S. political system, including the 2016 U.S. presidential election," noted the indictment.[17] The Russians employed social media to attack the presidential candidates that they (along with most American experts) considered strongest, while ignoring their apparently weaker challengers. Russian agents allegedly

> *engaged in operations primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump. . . . On or about February 10, 2016, Defendants and their co-conspirators internally circulated an outline of themes for future content to be posted to [Internet Research Agency]-controlled social media accounts. Specialists were instructed to post content that focused on "politics in the USA" and to "use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)."*[18]

The efforts of these operators received supporting fires, as it were, from leaks of embarrassing e-mails exfiltrated by Russian intelligence from the headquarters of the Democratic Party and released to the news media in increments to distract Clinton's campaign.[19] A month before the election, the secretary of homeland security with the director of national intelligence jointly explained to the world that the "Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations." The disclosures resembled "the methods and motivations of Russian-directed efforts"; indeed, "the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there." Secretary Jeh Johnson and Director James Clapper assessed that with "the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities."[20] After the election, a team of experts convened by the Center for Strategic and International Studies in Washington concluded that Russia had "invested in a systematic, multi-year campaign to not merely affect the results of an individual election, but sow chaos and undermine trust in the liberal democratic order itself."[21]

As the world saw in the US 2016 election, such targeting of individuals and societies via the "information space" could have strategic effects.

As the world saw in the 2016 election, such targeting of individuals and societies via the "information space" could have strategic effects by eroding the cooperation necessary to sustain a democratic society. This thought has impressed leaders in Europe as well. It made the French wary. Russian actors followed the same playbook to sabotage the candidacy of Emmanuel Macron in France's spring 2017 presidential race, and though they dumped thousands of Macron's campaign emails on the public two days before the election, Macron's cyber savvy campaign limited their intrusions and the resulting damage.[22]

British leaders that same year nevertheless cited in public a growing threat of Russian cyber and electoral disruption potentially backed by powerful military forces. Prime Minister Theresa May warned in November 2017 that Moscow had "mounted a sustained campaign of cyber-espionage and disruption."[23] Its tactics, she claimed, "included meddling in elections." A few days later, Ciaran Martin, chief of Britain's new National Cyber Security Centre (NCSC), accused Russia of "seeking to undermine the international system."[24] Attribution is not proof, as noted above, but if a victim state ties itself up in arguments over the standards of proof that a response should require, then that state is hardly acting decisively. Which is perhaps the point.

Interestingly, the US Congress looked at this situation and decided that responding to such provocations could <u>not</u> be done exclusively through covert action. What was required would have to include military action in cyberspace, as noted above. That change gains relevance when read with a later section in the same FY19 National Defense Authorization Act. Section 1642 covers "Active defense against the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and Islamic Republic of Iran attacks in cyberspace," and offers the president the authority to order US Cyber Command "to disrupt, defeat, and deter cyber attacks" by nations that conduct "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes."[25]

A related question: Can cyber operations covertly unite as well as divide? Yes, they can and do. That is precisely its danger to regimes. It allows outside influences to reach directly inside a country to talk to that country's citizens and turn them against the regime. Hence the fear of many autocracies and their herculean efforts to establish and guard their "virtual borders." This is not clandestine diplomacy, but it is the same principle. When the Islamic State in Syria and the Levant (ISIL) took to the internet, Western leaders and security services feared what their citizens might see there.[26] ISIL's "caliphate" by early 2015, for example, offered websites and slick online magazines, in addition to posting the names, photos, and addresses of dozens of US military personnel, and calling on supporters to attack them in America.

This was personal targeting in the extreme, designed to turn at least a few neutral but persuadable Muslims in the West against their adoptive homelands.[27] ISIL did not manage to reach any of the service members named in the online postings, but its various exhortations still prompted attacks in Garland, Texas, and San Bernardino, California. In the latter, a husband-and-wife team shot up an office holiday party before dying in a suburban firefight with police in which the two sides exchanged more than 500 shots.[28]

Conclusion

The argument here is not that all offensive cyberspace operations should (or should not) be labeled and overseen as covert action. Rather, the technology of cyberspace seems to

Rather, the technology of cyberspace seems to be producing something unexpected: operations and effects that resemble covert actions but are much larger in their scale and reach.

be producing something unexpected: operations and effects that resemble covert actions but are much larger in their scale and reach. If covert action represents one way to bridge the gap between diplomacy and war, then cyberspace operations might offer another span, as it were, for exerting influence. Social media trolls do not have to rig an election to succeed; they just have to get Americans (or Britons, for Frenchmen . . . .) arguing with each other. ISIL does not have to inspire more than a handful of “lone wolves” in the West to spread fear of Muslims and fuel bitter debates over immigration. Success in covert action tends to prompt imitation, at least until the would-be victims learn to prevent such tactics (or find ways of setting norms to tame them). The signs, as seen above, do not look promising, for the arguments over attribution, response, and collusion do not seem to be receding.

At the same time, however, the affinities between “covert cyber action” and the quiet signaling described by Len Scott and Austin Carson above suggest new avenues for inquiry into what is happening in the cyber domain. This is an open field for scholarship into how states explicitly and tacitly bargain with one another in and through cyberspace. There is a great deal of ambiguity remaining about covert action, particularly over its place in cyberspace and its differences from traditional military and diplomatic activities. Such work should be informed not only by international relations theory but also by the history of intelligence, which amply shows that covert action works in the shadows to split an adversary’s “seams.”

❖ ❖ ❖

The author: Michael Warner is a historian with the US Department of Defense. He wishes to thank Josh Rovner and Kristian Gustafson, whose insights helped refine the analysis here.

❖ ❖ ❖

Endnotes

1. Adda Bozeman, “Political Intelligence in Non-Western Societies: Suggestions for Comparative Research,” in Roy Godson, ed., *Comparing Foreign Intelligence: The US, the USSR, the UK, and the Third World* (Pergamon-Brassey’s, 1988), 147–49.
2. Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton University Press, 2018), 3–6, 268.
3. Intelligence Authorization Act for Fiscal Year 1991 (P.L.102-88), sec. 503e; accessed January 14, 2019; https://www.congress.gov/bill/102nd-congress/senate-bill/1325/text.
4. 50 US Code, sec. 3093e.
5. Len Scott, “Secret Intelligence, Covert Action and Clandestine Diplomacy,” in LV Scott and PD Jackson, eds., *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (Routledge, 2004), 169–74.
6. Kristian Gustafson, “Direct Political Repercussions: Clausewitzian Philosophy and Covert Action,” presented at the International Studies Association Conference, Toronto, March 2019.
7. Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (University of Georgia Press, 2016), 61–62.
8. Sun Tzu, *The Art of War*, Chapter 3. Emphasis added.
9. Gustafson, “’Direct Political Repercussions’: Clausewitzian Philosophy and Covert Action,” 8. Quoted with the author’s permission.
10. R. Harris Smith, *OSS: The Secret History of America’s First Central Intelligence Agency* (University of California Press, 1972), 115–22. Rick Atkinson, *The Day of Battle: The War in Sicily and Italy, 1943–1944* (Henry Holt, 2008), 187–89.
11. Brantly, *The Decision to Attack*, 62.
12. William Robert Carruthers, “Covert Action and Cyber Offensive Operations: Revisiting Traditional Approaches in Light of New Technology,” unpublished Ph.D. dissertation, University of Salford, School of Arts and Media, 2018, 30, 153–54.
13. Brantly, *The Decision to Attack*, 62.

14. Brandon Valeriano and Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” Cato Institute, Policy Analysis No. 862, January 15, 2019; accessed February 7, 2019 at https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint
15. Jon R. Lindsay and Erik Gartzke, “Coercion through Cyberspace: The Stability-Instability Paradox Revisited,” in Kelly M Greenhill and Peter Krause, eds., *Coercion: The Power to Hurt in International Politics* (Oxford University Press, 2018), 202.
16. Robert S. Mueller, III, *US Department of Justice, Report on the Investigation Into Russian Interference in the 2016 Presidential Election* (“the Mueller Report”), Vol. I, March 29, 2019, pp. 14-15; accessed August 8, 2019 at https://www.justice.gov/storage/report.pdf
17. United States of America v. Internet Research Agency et al., US District Court for the District of Columbia, February 16, 2018, 3; accessed February 17, 2018 at https://www.scribd.com/document/371718383/Internet-Research-Agency-Indictment-pdf#from_embed
18. Ibid, p. 17. See also Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” *New York Times*, November 1, 2017, accessed February 19, 2018 at https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html
19. Mueller Report, Vol. I, 36–45.
20. “Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security,” October 7, 2016; accessed February 26, 2018 at https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.
21. Suzanne Spaulding and Eric Goldstein, *Countering Adversary Threats to Democratic Institutions: An Expert Report* (Center for Strategic and International Studies, 2018), 2; accessed October 26, 2018 at https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.
22. Heather A. Conley and Jean-Baptiste Jeangène Vilmer, *Successfully Countering Russian Electoral Interference*, (Center for Strategic and International Studies, 2018); accessed February 12, 2019 at https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.
23. “Theresa May accuses Vladimir Putin of election meddling,” BBC, November 14, 2017; accessed February 26, 2018 at http://www.bbc.com/news/uk-politics-41973043.
24. “UK cyber-defence chief accuses Russia of hack attacks,” BBC, November 15, 2017; accessed February 26, 2018 at http://www.bbc.com/news/technology-41997262.
25. See the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No: 115-232, Secs. 1632 and 1642, specifically the former’s provision that “(c) Clandestine activities or operations.—A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).”; accessed January 27, 2019 at https://www.congress.gov/bill/115th-congress/house-bill/5515/text#toc-HE880465A6D374869BD787DE7F19B0016.
26. Emerson T. Brooking and P. W. Singer, “War Goes Viral: How social media is being weaponized across the world,” *The Atlantic*, November 2016; accessed February 24, 2018 at https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125
27. Michael S. Schmidt and Helene Cooper, “ISIS Urges Sympathizers to Kill U.S. Service Members It Identifies on Website,” *New York Times*, March 21, 2015; accessed June 21, 2015 at http://www.nytimes.com/2015/03/22/world/middleeast/isis-urges-sympathizers-to-kill-us-service-members-it-identifies-on-website.html?smid=fb-nytimes&smtyp=cur&bicmp=AD&bicmlukp=WT.mc_id&bicmst=1409232722000&bicmet=1419773522000&_r=1.
28. Rick Braziel, Frank Straub, George Watson, and Rod Hoops, *Bringing Calm to Chaos: A Critical Incident Review of the San Bernardino Public Safety Response to the December 2, 2015, Terrorist Shooting Incident at the Inland Regional Center* (US Department of Justice [Office of Community Oriented Policing Services], 2016), 40; accessed February 20, 2018 at http://ric-zai-inc.com/Publications/cops-w0808-pub.

❖ ❖ ❖