Fall 9-18-2020

Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention (Originally published as part of the Hoover Institution's Aegis Series)

Gary Corn
American University, Washington College of Law, gcorn@wcl.american.edu

Fall 9-18-2020

Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention

Gary Cor

A HOOVER INSTITUTION ESSAY

Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention

GARY P. CORN

Aegis Series Paper No. 2005

> *All warfare is based on deception.*[1]
>
> *It clearly follows from the liberty and independence of Nations that each has the right to govern itself as it thinks proper, and that no one of them has the least right to interfere in the government of another.*[2]

If information is power, then the corruption of information is the erosion, if not the outright usurpation, of power. This is especially true in the information age, where developments in the technological structure and global interconnectedness of information and telecommunications infrastructure have enabled states to engage in malicious influence campaigns at an unprecedented scope, scale, depth, and speed. The Digital Revolution and the attendant evolution of the global information environment have intensified, if not generated, what one expert describes as "one of the greatest vulnerabilities we as individuals and as a society must learn to deal with."[3] The relative explosion of digital information and communications technology (ICT) and the modern information environment it has enabled "have resulted in a qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation."[4]

As evidenced by Russia's recent efforts at election interference in the United States and Europe, the role of information conflict in global strategic competition has evolved and taken on new weight.[5] A number of revisionist states, Russia and China chief among them, have fully embraced the new reality of the modern information environment, deftly adapting their capabilities and strategies to exploit the societal vulnerabilities it exposes. They have incorporated sustained, hostile influence campaigns as a central part of their destabilizing strategies to cause or exacerbate societal divisions, disrupt political processes, weaken democratic institutions, and fracture alliances, all with a broader aim of undermining the rules-based international order and gaining competitive advantage.

The anchor for these campaigns is the extensive and deep use of ICTs to conduct covert deception and disinformation operations at an extraordinary scale. Deployed at a strategic

---

The opinions expressed herein are those of the author and do not necessarily reflect the views of the Department of Defense or any other organization or entity with which the author is affiliated.

level, malign influence and disinformation operations have the very real potential to undermine and disrupt a targeted state's independent exercise of core governance prerogatives. Along with the advent of hostile cyber operations, these ICT-enhanced deception campaigns have raised challenging questions about whether and how international law applies to these novel state interactions. This paper focuses on the customary international-law prohibition against intervening in the internal and external affairs of another state—a rule intended to protect the cardinal right of states to conduct their affairs without outside interference. It considers the rule's applicability to the murky and evolving landscape of information conflict. Drawing on general principles of law, it argues for an interpretation of the nonintervention rule better suited to the realities of the information age, where undermining the exercise of sovereign free will is the specific aim of strategic covert deception and disinformation campaigns.

The nonintervention rule is important because US adversaries see the information environment as fertile ground for subverting the United States and the rules-based international order. Among the reasons for this perspective is the tremendous ambiguity surrounding the international legal framework applicable to states' use of ICTs, especially in the gray zone below traditionally recognized use-of-force thresholds and outside of armed conflict. To date, efforts to achieve greater clarity regarding international law's applicability to states' use of ICTs, whether led by states or otherwise, have focused almost exclusively on the problem of harmful cyber-effects operations—the use of cyber capabilities to disrupt, deny, degrade, destroy, or manipulate computers or information systems or the data resident thereon. With the exception of some limited scholarship and commentary on the international-law implications of Russia's 2016 election interference, little work has been done to analyze the use of ICTs as a platform for covert deception.

The primary conflict-regulation mechanism in international law is the United Nations (UN) Charter prohibition on states using force against the political independence or territorial integrity of other states. While a small number of states have recently signaled a willingness to consider some cyber operations involving serious financial or economic harm as amounting to uses of force, they have thus far not indicated the same openness with regard to influence operations. For good reason, they are unlikely to do so. Overly expansive invocation of the use-of-force prohibition has obvious escalatory implications. In contrast, the nonintervention rule, which governs both forcible and nonforcible measures, is far more suited to regulating the sub-use-of-force threats the nuanced sphere of information conflict and covert deception pose.

With respect to cyber-effects operations, there is little if any dissent from the view that the rule of prohibited intervention applies to states' use of ICTs.[6] Consensus quickly breaks down, however, over the rule's content. The rule is generally described as prohibiting coercive measures against a limited but important zone of sovereign interests falling within what is commonly referred to as a state's *domaine réservé*. Unfortunately, substantial

definitional and conceptual uncertainty clouds understandings of the "elements" of this rule and how they apply in practice, especially in the context of cyber and information conflict. The International Court of Justice (ICJ) has described the element of coercion as "defin[ing], and indeed form[ing] the very essence of, prohibited intervention."[7] Many commentators have treated this statement as canonical and have applied it dogmatically, notwithstanding the court's failure to offer a definition of the term. Both the ICJ's statement and the undue weight many afford it misapprehend the true objective of the rule—to prevent states from employing measures aimed at depriving a targeted state of the free exercise of its will over protected sovereign matters. They also fail to capture significant modes of state action, strategic covert deception in particular, that should be considered internationally wrongful.

As the attorney general of the United Kingdom has noted, achieving greater clarity as to the nonintervention rule's force and effect is of "particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections."[8] Adapting the concept of coercion to account for the realities of modern information conflict is a necessary step toward achieving the clarity he seeks. Deception is frequently regulated in domestic legal regimes, either directly in the form of criminal fraud provisions, or indirectly through the recognition that deception can substitute constructively for the actual force and coercion elements of other crimes. In both cases, it is the subversion of free will that is considered the cognizable harm. States should draw on these general principles of law to inform the concept of coercion in international law and thereby better define the nonintervention rule's applicability to information conflict.

This paper's efforts to reinforce the existing international legal architecture are not offered as a panacea to the ill of foreign influence campaigns. International law has its limits, and countering hostile foreign influence will require a far more holistic and concerted approach than simply evolving or achieving greater clarity as to the scope of applicability of any particular rule of international law. But as one important study notes, the United States "needs an updated framework for organizing its thinking about the manipulation of infospheres by foreign powers determined to gain competitive advantage."[9] The US Department of Defense's implementation of a new cyber strategy in 2018 with its operational concept of "defend forward" is a step in the right direction, as evidenced by the success of US Cyber Command's reported operations to counter Russian election interference in 2018. Accurately characterizing covert influence campaigns as a matter of international law would add additional tools to the defend-forward toolbox, and doing so should figure prominently in a broader effort to develop a coherent strategy and framework to counter foreign influence efforts while reinforcing the rules-based international order.

The Problem: Covert Deception and Disinformation Operations at Scale

Information conflict is not new. Propaganda is a truly ancient human endeavor, and states have leveraged information—truthful, manipulated, and fabricated—for influence purposes since the inception of the Westphalian order. Hostile influence campaigns have historically

assumed many monikers and taken many forms but generally share the common characteristic of disseminating overt and covert propaganda (including facts, opinions, rumors, half-truths, and lies) in pursuit of a competitive advantage over an opponent. Suasion, including the use of propaganda, is a staple of statecraft and has long been viewed as falling outside international law's reach.

The Cold War provides a relatively recent example. Political warfare was the defining characteristic of the conflict, and a primary weapon in the Soviet Union's arsenal was its use of "active measures"—subversive practices including political influence efforts, the surreptitious use of Soviet front groups and foreign communist parties, and the core element of *dezinformatsiya* (disinformation).[10] One former KGB general described the use of active measures as "the heart and soul of the Soviet intelligence" apparatus, specifically designed to subvert the United States and "drive wedges" in the West's alliances.[11] To be sure, the United States also employed deception during the Cold War. But Russia has reinvigorated such efforts in the post–Cold War era; according to recent US intelligence assessments, Russia's campaign to interfere in the 2016 presidential election "demonstrated a significant escalation in directness, level of activity, and scope of effort" to undermine "the U.S.-led democratic order."[12]

Russia's efforts in 2016 were aimed directly at the US presidential election. The objective was to undermine public faith in the democratic process and to denigrate and harm the electability of one candidate and boost the candidacy of another. Although unprecedented in scope and scale, Russia's campaign "followed a longstanding . . . messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"[13] Russia employed a multifaceted approach to its interference campaign that involved cyber espionage against both political parties; the weaponization of sensitive information collected through those operations, specifically the timed release through intermediaries of personal emails and other damaging information belonging to Democratic Party officials and political figures; hacking into state and local electoral boards and voting systems; and a deep and extensive propaganda effort, both overt and covert.[14]

Russia's use of "quasi-government trolls" to covertly propagandize and spread mis- and disinformation played a central role in its election interference efforts and demonstrated Russia's broader goals of undermining public faith in the democratic process and institutions and generally seeding and cultivating political discord. The Internet Research Agency (IRA), an entity in St. Petersburg, Russia, financed by a Russian oligarch and close Vladimir Putin ally with ties to Russian intelligence, ran an extensive and well-organized social-media *dezinformatsiya* campaign.[15] Among other tactics, the IRA used false personas and the stolen identities of real Americans to purchase millions of dollars' worth of advertising on social media platforms such as Facebook, Twitter, and Instagram to plant propaganda, and used false accounts and bots to amplify its messaging. The IRA also used

these false social media accounts to stage political rallies in the United States and to solicit and pay unwitting US persons to promote or disparage candidates.

Based on these well-documented interference efforts, in 2018 the grand jury in Special Counsel Robert Mueller's investigation returned an indictment of thirteen Russian individuals and three companies associated with the covert deception campaign.[16] Each was accused, inter alia, of conspiring "to defraud the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purposes of interfering with the U.S. political and electoral process, including the presidential election of 2016."[17] The indictment lays out in detail the IRA's, and by extension Russia's, extensive covert influence activities aimed at swaying the 2016 election and "sow[ing] discord in the U.S. political system."[18] In 2020, the Senate Select Committee on Intelligence released an extensive three-volume report, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, confirming the intelligence community's assessment.[19]

Russia's interference and covert influence campaigns are not limited to targeting the United States. Europe has been on the receiving end of Russia's disruptive efforts perhaps longer than has the United States.[20] In addition to targeting an array of European states with destabilizing disinformation campaigns generally, Russia has targeted elections in Ukraine, France, Germany, and the United Kingdom, to name a few, as well as the European Parliament election in 2019.

Russia's interference in the 2016 presidential election served as a wake-up call. In response, the United States mounted a concerted, government-wide effort to protect the 2018 midterm elections against Russian interference operations, taking measures that reportedly included Department of Defense cyber operations. But Russia's covert influence operations have not abated. All indicators point to Russia stepping up its efforts to interfere in the 2020 elections.[21] Evidence is also mounting that Russia is disseminating disinformation regarding the COVID-19 pandemic in order "to aggravate the public health crisis in Western countries, specifically by undermining public trust in national healthcare systems—thus preventing an effective response to the outbreak."[22]

Russia is not alone in this regard. Although arguably several steps behind, China has also moved aggressively into the information conflict arena. The Chinese Communist Party "has used ideology and propaganda as governing tools 'since the People's Republic was established in 1949,' and this can even be dated to the Party's founding in 1921."[23] While traditionally these efforts were more internally focused, China now views influence and information operations as a "magic weapon" for achieving its foreign policy goals.[24] Indications are that it has learned from Russia's disinformation campaigns. China is testing those lessons and refining its influence capabilities in Taiwan and Southeast Asia and has moved beyond spreading, for example, COVID-19–related disinformation.[25]

Russia and China present the most advanced information-conflict threats, but they are not the only threats. Iran and other US adversaries are studying, emulating, and adapting the Russian and Chinese models to advance their own disruptive goals. According to the 2019 Worldwide Threat Assessment, "US adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere."[26] In each case, these campaigns extend beyond open influence activities, employing sophisticated deception operations to achieve strategic aims. Countering these efforts is and should be a stated US policy goal, along with strengthening the international rules-based order and the applicability of international law to states' use of ICTs, other emerging technologies, and interactions in the information environment.[27] The rule of prohibited intervention is the most pertinent rule of international law available to confront the harm of election interference and covert deception campaigns.

International Law and the Principle of Nonintervention

State sovereignty and the principle of sovereign equality form the foundation upon which the rules-based international order rests.[28] At its core, sovereignty signifies independence in relations between states, with independence being the right to exercise the functions of a state within a defined portion of the globe—the territory under the state's lawful jurisdiction—to the exclusion of any other state.[29] These organizing principles underlie the most important rules of international law governing interstate relations, such as the *jus ad bellum* prohibition on states using force against the territorial integrity or political independence of other states.[30]

States have also developed the customary international-law principle of nonintervention as a safeguard against impairments of their sovereignty. The principle is considered a "corollary of every state's right to sovereignty, territorial integrity and political independence."[31] It protects the "right of every sovereign State to conduct its [internal and external] affairs without outside interference."[32] The nonintervention principle is written into numerous international instruments, and states frequently invoke it, albeit with imprecision and under disparate circumstances.

The customary status of the nonintervention rule is not controversial, and the proposition that it applies to states' use of ICTs, at least in the context of cyber operations, is gaining increased acceptance among states.[33] Further, it is widely recognized that the rule can be violated by both forcible and nonforcible means.[34] Unfortunately, outside of relatively clear examples of forcible interventions—which concurrently violate the prohibition on the use of force—the rule's content is commonly recognized as ill defined.[35] This makes it difficult to discern the line between nonforcible but unlawful interventions on the one hand and lawful influence activities on the other.

States routinely employ various means of statecraft with the intent of shaping other states' policy decisions or actions, and there is no general prohibition in international law against

states engaging in suasion. And although states frequently invoke the terms intervention and interference to complain about such activities, they are not the same normatively. International law only proscribes the former as wrongful; "interference pure and simple is not intervention."[36] It is an important distinction, setting apart what states view as legitimate from illegitimate forms of statecraft, itself an expression of sovereign will. Unfortunately, the indeterminate line between mere interference and prohibited intervention weakens the nonintervention rule's value as a guard against impairments of sovereign rights and "risks permitting coercive policies that undermine the political independence of states or impair the right to self-determination," especially in the context of information conflict.[37]

Although the precise content and scope of the nonintervention principle are unclear, certain core aspects of the rule are evident. The general contours can be gleaned from the ICJ's description of the principle in its *Nicaragua* judgment, where it explained:

> The principle [of nonintervention] forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[38]

This passage is often cited for the proposition that interference is only internationally wrongful when two constituent elements are present. First, the measures employed must be directed against the *domaine réservé* of the targeted state. Second, such measures must be coercive.[39]

The ambiguity that plagues the nonintervention rule generally also infects these two elements. Unfortunately, the ICJ has offered little by way of additional explanation. This should not be surprising. The court's discussion of nonintervention in the *Nicaragua* judgment was narrowly confined to the specific facts of the case, which primarily concerned forcible measures.[40] Further, the court's entire *sua sponte* discussion of the nonintervention principle was only for the purpose of ruling out whether the forcible measures attributed to the United States were justified as countermeasures.[41] As such, its broader pronouncements on the elements of the rule—or lack thereof—were unnecessary and should be considered with circumspection.[42] Still, convention holds that the concept of coercion demarcates the line between mere interference and wrongful intervention.[43]

The ICJ's focus on coercion as the touchstone of prohibited intervention likely reflects the evolution of the rule over time from one that traditionally served to protect only the

territorial integrity of states against military force to one aimed at also shielding political independence against nonforcible infringements.[44] In this regard, the term is perhaps equally inapt and unhelpful since in common parlance the concept of coercion is generally considered to involve force or the threat of force to impose one's will on another.[45] As set out below, overreliance on coercion as a defining element of intervention distorts the focus of the rule and risks excluding from its scope nonforcible means of subverting protected sovereign interests. Before turning to the element of coercion, however, a brief discussion of the concept of *domaine réservé* is useful.

The Concept of *Domaine Réservé*

As noted, the nonintervention rule does not reach all forms of state interference in the internal affairs of other states. It is a rule of finite scope as to both the object and means of outside state action. And states have generally rejected proposals to prohibit their use of propaganda to influence other states. With respect to the object of prohibited intervention, the zone of sovereign interests or state functions protected by the rule has never been well understood or defined.

Oppenheim describes intervention generally as "a form of interference by one state in the affairs, internal or external, of another" by either direct or indirect means.[46] By "affairs," Oppenheim is referring loosely to the prohibited object of intervention—matters which, as a function of sovereignty, are reserved in international law to the sole prerogative of states. This zone of protected interests is often referred to, imprecisely, as the state's *domaine réservé*. As Jens David Ohlin has noted, "despite the patina of precision in its French rendering, the concept has little internally generated content" as a concept.[47]

Strictly speaking, *domaine réservé* refers only to matters within a state's internal jurisdiction, and therefore does not speak to the full range of protected sovereign functions which also include a state's external affairs.[48] According to the ICJ, these matters include, but are not limited to, the right to choose a political, economic, social, and cultural system and to formulate and execute foreign policy.[49] The right of states to independence over these matters is not conferred by international law, but rather is inherent in the concepts of statehood and sovereignty. Therefore, the rule's protection is better understood as extending to those matters in which each state has the right, "by the principle of State sovereignty, to decide freely."[50] Restrictions on states' independence over these sovereign matters cannot be presumed.[51]

Perhaps the most frequently cited example of a matter falling within the scope of the *domaine réservé*, and thus within the nonintervention rule's protection, is a state's choice of both its political system and its organization.[52] In contrast, purely commercial government activities are generally considered to fall outside of the *domaine réservé*.[53] Between these extremes, uncertainty lingers, and the rule's scope depends on a number of variables, including, perhaps most importantly, the degree to which a particular state's discretion

over a matter is subject to its specific international obligations. To the extent a state's policy choices are governed by international law, the state is considered to have surrendered its discretion over the matter. That is, the concept of sovereign prerogative is not without limits, and those "domains or activities" not strictly reserved to the state are said to be potentially subject to foreign action.[54] Accordingly, in light of the ever-expanding subjects of international regulation, some commentators argue that the concept of *domaine réservé* is diminishing, and therefore so too is the utility of the nonintervention rule.

These are exaggerated claims. First, since international legal obligations vary from state to state, the "margin of liberty" each exercises will differ accordingly.[55] International legal obligations differ widely as to content and may apply differently depending on the state involved and the given circumstances. Further, states often retain significant independent authority even with respect to matters committed to international law.[56] The scope of another state's authority to intervene in a matter regulated by international law will generally be defined by the source of the obligation at issue. Most often, available remedies are narrow and specifically defined in applicable treaties. Outside of such treaty-based measures, the customary law of state responsibility sets a high bar for an intervening state to claim that the wrongfulness of its employment of coercion against a targeted state should be excused or precluded as a legitimate countermeasure.[57] Therefore, the fact that a matter is in some way the subject of international regulation does not equate to a license for other states to coerce decisions or conduct with respect thereto.

Ultimately, like many aspects of international law, whether a matter falls within the protective ambit of the nonintervention rule involves a fact-specific inquiry, considering state practice and *opinio juris* prevalent at the time.[58] Suffice to say that, notwithstanding the increasing degree to which states surrender some degree of sovereignty to international regulation, there exists a strong presumption that matters of state governance fall to the sole prerogative of states and are protected from external intervention. That is, "it is in the expression of [the] idea" that sovereignty equates to "the exclusion of the authority of other states, but not international law," that "the principle of nonintervention has its primary function."[59] Holding elections and implementing public-health measures, two areas that Russia has specifically targeted in the last several years, certainly fall within this protective umbrella. Elections are frequently cited as a quintessential matter falling within a state's *domaine réservé*.[60] Similarly, the adoption and implementation of public-health policies and measures, especially in the face of a global pandemic, are widely recognized as legitimate matters of governance within a state's internal sovereign jurisdiction.[61]

The Elusive Element of Coercion

As with the concept of *domaine réservé*, little interpretive guidance exists in international law regarding the element of coercion. In *Nicaragua*, the ICJ described as a particularly obvious case "an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another

State."[62] Equally obvious is that neither propaganda nor aggressive diplomacy qualifies as a prohibited intervention, at least not per se.[63] Between these extremes, the standard lacks clarity, making it difficult to map to the realm of information conflict.

The principle of nonintervention has been described as a "doctrinal mechanism to express the outer limits of permissible influence that one state may properly exert upon another."[64] Since the principle's inception, locating the demarcation between permissible and impermissible influence has proved exceedingly difficult. The vagueness in the rule's scope and meaning traces back to the principle's conceptual roots and the differences in the early naturalist and positivist approaches to international law generally, and to the principle's definition and evolution specifically—differences beyond the scope of this paper.[65] It is enough to note that a significant aspect of these early debates centered on whether the principle was absolute or was subject to exception, for example, as a matter of self-preservation.[66] The latter view ultimately held sway, shifting the focus of the debate to the issue of when interventions might be justified, and, more important to the present discussion, how to define the "outer limits" of permissible influence.

Historically, armed force, described as "dictatorial interference," was considered the dividing line between permissible and impermissible influence.[67] In fact, well into the twentieth century, many states and commentators, including the United States, held the view that prohibited intervention and the prohibition on the threat or use of force were equivalent.[68] Over time, however, the concept of intervention expanded, and coercion evolved as a broader but inapt benchmark for denominating the boundary between lawful influence and prohibited intervention.

Thus, according to Oppenheim, "to constitute intervention [an] interference must be forcible or dictatorial, *or otherwise coercive*," and can take the form of direct or indirect military action, as well as nonmilitary actions such as economic or political measures "where they have the necessary coercive effect."[69] This expanded concept of intervention also finds expression in a number of treaties, declarations, and General Assembly resolutions concluded in the latter half of the twentieth century—instruments that the ICJ has cited as reflective of customary international law.[70] For example, the Friendly Relations Declaration recalls "the duty of States to refrain in their international relations from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of any State."[71] However, beyond reinforcing the notion that prohibited interventions can be effected by nonforcible means, these sources offer little guidance on the meaning of *coercion* as the term is used in the specific context of intervention, and in certain respects are at odds with state practice. States routinely use sanctions and other economic means to pressure or compel other states and have frequently rejected proposals that would deem the use of economic pressure as internationally wrongful.

The ICJ's rendering of the nonintervention principle in its *Nicaragua* judgment is often cited as offering a definitive description of the rule's content. According to the court:

> Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[72]

However, as noted above, the court specifically limited the scope of its review, confining its description to "only those aspects of the principle which appear to be relevant to the resolution of the dispute."[73] By and large, the dispute was over measures the court separately determined to constitute direct and indirect uses of force that it deemed "particularly obvious" examples of intervention.[74] Beyond this discussion, the court intimates that coercion can involve nonforcible measures, but offers no guidance on how.

Undue weight is often ascribed to the court's discussion of the nonintervention rule. Its account of the rule is nonbinding and general in description.[75] In this regard, its comment that coercion "defines" and "forms the very essence" of the rule is overbroad and misleading. As set out below, the essence of the nonintervention rule is the prevention of measures intended to subvert a state's independence over protected sovereign prerogatives, or free will. The court's reference to coercion is better understood as illustrative of the fact that not all modes of interference are internationally wrongful, and a loosely conceived concept of coercion specific to the nonintervention context has emerged over time as a reference point for distinguishing between permissible and impermissible influence.[76]

Defining a sensible limit to the principle's reach is no doubt important; otherwise the rule risks sweeping within its ambit "any act which ha[s] an effect on another state."[77] However, overinclusiveness is not currently the problem. As reflected in the ICJ's emphasis in *Nicaragua* on the concept of coercion, the nonintervention rule is mired in the past and therefore tethered to force as the sine qua non of its violation. This raises legitimate questions as to the rule's utility in light of the separate prohibition on the use of force. And while there is general agreement that the rule now comprehends nonforcible modes of coercion, what that means in practice remains clouded in uncertainty. Owing to the historical force-prohibition emphasis of the rule, efforts to elucidate the meaning of coercion frequently miss the mark on correlating this "element" to the underlying purpose of the nonintervention principle—to protect against the subversion of a targeted state's independent sovereign choices—making underinclusiveness a far greater risk. This dynamic has become particularly evident in the context of information conflict.

Some also consider the *Nicaragua* judgment to imply that to constitute coercion, one state's actions must involve an actual threat against the affected state, and the threatened

consequence of noncompliance must itself be unlawful.[78] However, nothing in the judgment or international law more broadly requires that an intervention be effected by threat of consequence, lawful or otherwise. To the extent that a threat is involved, the threatened consequence must be judged contextually to determine whether it crosses the line between prohibited coercion and lawful, albeit "corrosive," pressure.[79] Furthermore, interpreting nonintervention as being premised on a compelled quid pro quo again misapprehends the interest protected by the rule—unimpeded sovereign prerogative and the right of independence in governance. As discussed further below, threats of negative consequence are not the only means for undermining this interest.

It is well recognized that the principle of nonintervention is an outgrowth, or corollary, of the principles of sovereignty and the sovereign equality of states. "Sovereignty in the relations between States signifies independence,"[80] and independence has long been understood as "the power of giving effect to the decisions of a will which is free" from external restraint.[81] Where a state employs measures "calculated to impose certain conduct or consequences" on a targeted state that if successful would "in effect [deprive] the state intervened against of control over [a sovereign] matter," the line between interference and intervention is implicated and likely crossed.[82] Nonintervention is far more about potential consequence than it is about the means employed. While the choice of means is a relevant factor, as in the case of forcible measures that are presumptively employed to compel an outcome, it is not definitive. Thus, the rule is better understood as prohibiting measures calculated and likely to deprive, subordinate, or substantially impair the right of independence in governance, and such interventions are wrongful even if inchoate or unsuccessful.[83]

In her recent Chatham House paper on sovereignty and nonintervention, Harriet Moynihan reaches a similar conclusion. She describes coercion as the application of pressure or compulsion by one state sufficient to subordinate the sovereign will of the targeted state.[84] Thus, in her view, "the non-intervention principle is in practice capable of broader application" than a narrow interpretation of the ICJ's description of coercion would suggest.[85] According to Moynihan:

> Sources [suggest] that the coercive behaviour could extend beyond forcing a change of policy to other aims, such as preventing the target state from implementing a policy or restraining its ability to exercise its state powers in some way. At the same time, as noted above, the attempt to deprive the target state of its free will over its sovereign powers is carried out for the benefit of the perpetrating state in some way: the unauthorized exercise of authority is not incidental. The benefit sought need not relate to a specific policy issue; it may suffice for the target state's control over the underlying policy area to be impaired in a way that adversely affects the target state. In light of this, the coercive behaviour is perhaps best described as pressure applied by one state to deprive the target state of its free will in relation to the exercise of its sovereign rights in an attempt to compel an outcome in, or conduct with respect to, a matter reserved to the target state.[86]

This approach correctly places emphasis on the nonintervention rule's central focus of protecting states' independence over core sovereign prerogatives.[87] Actions calculated to subvert a state's free will undermine the sovereign equality of states and the international order, and present a direct threat to international stability, peace, and security.

The Tallinn Manual 2.0 appears to take a similar approach. Rejecting the idea that coercion requires physical force, the manual states that coercion "refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[88] Not surprisingly, Michael Schmitt, the general editor, also recognizes that the primary focus of the nonintervention rule and the "core" function of the element of coercion is to prevent subordination of sovereign free will. In his view, "a coercive action is intended to cause the State to do something, such as take a decision that it would otherwise not take, or not to engage in an activity in which it would otherwise engage."[89]

The evolving realm and nature of information conflict is providing states with lucrative opportunities to undermine the sovereign decisions of adversaries, yet how the nonintervention principle applies to propaganda and influence campaigns remains unclear. Debates over whether Russia's reported hack into the Democratic National Committee's (DNC) servers and subsequent "meddling" in the 2016 presidential election constituted a prohibited intervention are a case in point. Some argue that, in the aggregate, Russia's actions sufficiently manipulated the election process to qualify.[90] Others view them as espionage and propaganda, which are not violations of international law by themselves, at least not per se.[91]

Some scholars and commentators considering the question of whether influence operations or propaganda alone can violate the rule have converged on the view that the use of covert deception crosses the intervention line, but little analysis is offered in support of this conclusion.[92] For example, Schmitt suggests that Russia's covert "troll" operation may have violated the nonintervention rule because "arguably, the covert nature of the troll operation deprived the American electorate of its freedom of choice" when exercising the franchise. But he does not elaborate on how this aligns with more rigid interpretations of coercion, such as those that would require an interaction premised on a threat of consequence.[93]

The answer is twofold. First, as set out above, the nonintervention rule has never been premised on the existence of a threat-based transaction. It is a rule meant to prevent states from engaging in measures calculated to subvert sovereign free will. Second, measures of deception are commonly recognized in domestic legal systems as cognizable harms precisely because they are a means of undermining the exercise of free will. States frequently regulate deception either directly in the form of fraud-based proscriptions, or indirectly by making deception a constructive substitute for force or coercion elements of other crimes. States can draw on these general principles to adapt the nonintervention rule to the realities of the modern information environment.

General principles of law common to the principal legal systems of the world are recognized as valid subsidiary sources for determining the scope and meaning of primary treaty and customary international-law rules such as the rule of prohibited intervention.[94] Admittedly, the means of identifying general principles of law and the normative weight to be accorded them is an open question, and a fulsome review of states' domestic legal regimes is beyond the scope of this paper.[95] What follows are illustrative examples with an emphasis on US domestic law. Like all states, the United States can draw on these principles to inform its views on the meaning of coercion as applied in the context of the nonintervention rule and, by extension, the scope of application of the rule more generally.

Deception as a Means of Undermining Free Will

The indictment of the thirteen Russians and three Russian organizations stemming from the special counsel's investigation into Russian election meddling in 2016 is a compelling exposition, albeit in the vernacular of US domestic law, of a prohibited intervention into the US electoral process. The indictment lays out in great detail Russia's extensive covert deception campaign intended to impair, obstruct, and defeat the lawful functions of the US government "for the purpose of interfering with the U.S. political and electoral processes."[96] Significantly, the gravamen of the indictment was that the Russians carried out their scheme of interference by nonforcible means of fraud and deceit.

Specifically, the defendants were charged, inter alia, with conspiring to defraud the United States in violation of 18 U.S.C. § 371 by impeding the lawful functions of the Federal Election Commission, the Department of Justice, and the Department of State to administer federal requirements for disclosure of foreign involvement in certain domestic activities.[97] Section 371, the general federal conspiracy statute, prohibits two or more persons from conspiring to obstruct or interfere with a legitimate government activity "by deceit, craft or trickery, or at least by means that are dishonest."[98] This portion of the statute is intended to "protect governmental functions from frustration and distortion through deceptive practices."[99] While cheating the government out of money or property can serve as one means by which someone can defraud the United States, prosecution under Section 371 is not limited to financial crimes.[100] Actions "calculated to frustrate the functions of an entity of the United States will suffice."[101]

The fraud provisions encompassed in Section 371 are not unique. They reflect long-standing common-law fraud concepts that proscribe both pecuniary and nonpecuniary harm, including depriving victims of a legal right. Fraud is also criminalized at the state level throughout the United States, and similar concepts can be found in the legal systems of most, if not all, nations. Fraud is a crime of deceit that traces its roots in both common and civil law systems to the early Roman *lex Cornelia de Falsis*.[102] Fraud and similar provisions recognize that deception can be both a means to a harmful end and a legally cognizable harm in and of itself.[103] As such, legal systems universally regulate deception directly by criminalizing fraud and other *crimen falsi*. Fraud and similar provisions are

ultimately grounded in the recognition that at its core, deception is a nonforcible means of undermining free will.

In addition to proscribing *crimen falsi*, legal systems commonly regulate deception indirectly as well, prescribing it as a constructive substitute for elements of actual force and coercion in other crimes. This legal principle has deep historical roots. For example, the common law has long recognized that for the crime of burglary, the element of breaking can be effected not just by actual force, but also constructively through deceit.[104] Constructive force is recognized in other areas of law as well: deception can substitute for force as the *actus reus* of larceny. Larceny by trick is a species of larceny dating back at least to 1779 in English common law,[105] where the element of trick substitutes for the wrongful-taking element required by larceny.[106] The rationale behind including larceny by trick within the crime of larceny is that "fraud vitiates the property owner's consent to the taking."[107] As such, the common law developed so that, to satisfy the requirements for larceny, "actual trespass or actual violence is not necessary. Fraud may take the place of force."[108]

Rape law offers another example of constructive force through deception. Although the traditional definition of rape required force or threat of force to satisfy the *actus reus*, the common law developed to embrace situations "in which the defendant employed deception rather than force."[109] Traditional common law distinctions between fraud in the factum and fraud in the inducement have steadily fallen away, with states trending toward adoption of the Model Penal Code approach, which states that consent is ineffective if "it is induced by force, duress or deception of a kind sought to be prevented by the law defining the offense."[110] Consistent with this trend, states have allowed specific instances of fraud in the inducement to serve as the basis for a rape conviction, including fraud in the context of certain professional relationships, spousal impersonation, impersonation of another, fraud as to the nature of the act, and "a few newer provisions more generally making consent obtained by fraud insufficient."[111] In each of these cases, the salient point is the recognition that deceit vitiates consent, the ultimate expression of free will.

Consider also the federal Trafficking Victims Protection Act (TVPA).[112] Passed as part of the Victims of Trafficking and Violence Protection Act of 2000, it was the first comprehensive federal law to address human trafficking. Recognizing that deception can "have the same purpose and effect" as actual threats of or use of physical coercion, Congress criminalized "severe forms" of human trafficking, which it defines as sex and labor trafficking induced by, inter alia, force, fraud, or coercion.[113] As one court recognized, "the TVPA not only protects victims from the most heinous human trafficking crimes, but also various additional types of fraud and extortion leading to forced labor."[114]

The idea that deception is a legally cognizable harm, in the form of fraud or as a constructive substitute for force or coercion, is not unique to United States law. These are precepts of law commonly reflected in domestic legal systems.[115] Drawing on these precepts,

some states have also begun passing legislation specifically addressing foreign influence, disinformation, and election interference.[116]

Australia, for example, passed comprehensive legislation in 2018 in response to the growing threat of foreign interference. As part of this legislation, the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 amended Australia's Criminal Code Act 1995 to create a slew of new criminal offenses related to national security, espionage, and foreign influence. The two most relevant offenses are general foreign interference and foreign interference involving a targeted person.[117] For purposes of these new offenses, Australia distinguishes between foreign influence, which it deems permissible, and foreign interference, describing the latter as conduct that "goes beyond the routine diplomatic influence that is commonly practised by governments [and] . . . includes covert, deceptive and coercive activities intended to affect an Australian political or governmental process."[118] This distinction tracks closely with general understandings of the divide between lawful interference and prohibited intervention in international law, and specifically recognizes covert deception as a means of intervention.

Australia is not alone in its efforts to combat foreign interference and adapt its domestic legal structure to account for the evolving nature of information conflict. France and other countries have either adopted or are considering laws to protect against foreign interference, disinformation, and election meddling. Many of these approaches similarly recognize the significance and threat of covert deception. These concepts are often reflected in international instruments as well. For example, Congress's approach to sex trafficking finds a direct analog in international law, which also recognizes that coercion need not be limited to physical force for purposes of human trafficking, defining trafficking to include inducement "by means of the threat or use of force or other forms of coercion, of abduction, of fraud, [or of] deception."[119] The war crime of prohibited perfidy, which is predicated on an act of treachery, offers another example of international law criminalizing deception, albeit under very narrow and particular circumstances.[120]

The foregoing examples are illustrative, not exhaustive. They demonstrate how deception operates as a legally operative harm with direct relevance to the principle of nonintervention. States can and should take account of these principles as legitimate subsidiary tools for elaborating the meaning of coercion in the context of nonintervention, better defining the scope of the rule, and adapting it to the realities of modern cyber and information conflict.

Calibrating the Pendulum

Applying these general principles to the element of coercion will better align the nonintervention rule with its underlying purpose and adapt it to the realities of the information age. As Sean Watts notes: "As States consider and weigh the merits and costs of various modes of interaction in the international system, charting options on this legal spectrum with some specificity becomes a prudent, if not always a simple exercise."[121] This

is notably true with respect to the increasingly complex dynamics of interstate relations in the cyber and information environments. States should leverage the nonintervention rule as a legitimate tool for deterring and regulating inimical action in these contexts.

Adopting the approach suggested here does not come without risk, however. Overbroad application of the rule would capture legitimate forms of statecraft and influence in its scope and raise collateral concerns regarding free expression that should be accounted for. States are rightfully unlikely to subscribe to a framework that sweeps too wide. Overt influence is a staple of international relations. It provides states an effective means of peacefully advancing their individual and collective interests on the world stage in a way that, even when aggressive, affords the targeted state the opportunity to contextualize and counter the influence in ways that covert deception campaigns are specifically intended to prevent. As Ohlin correctly asserts: "There must be a line between being coercive and being corrosive to the proper functioning of a democracy."[122] Clarifying how best to identify where that line falls is one thing. Blurring it further or erasing it altogether is another. Recognizing covert deception and disinformation campaigns as qualitatively and normatively distinct from overt influence, and as such a means of actual or constructive coercion, is a necessary step in drawing that line. However, additional limiting principles are warranted.

It is important to reemphasize at this point that to be wrongful, like any means or method of statecraft, covert deception must be intended "to influence outcomes in, or conduct with respect to, a matter reserved to a target State."[123] Clarifying or recasting the meaning of coercion would have no impact on defining the object of the rule's protection—states' *domaine réservé*. It would simply place the emphasis back on the ends that the principle of nonintervention is concerned with, with less dogmatic focus on the means employed. Ultimately, whatever means are employed, they "must have the potential for [actually or constructively] compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action that it would otherwise take)."[124]

Noting that coercion might fall along a broad spectrum from minimally invasive to "exceptionally aggressive" actions, any of which might or might not amount to intervention, Watts, borrowing from McDougal and Feliciano, proposes a test of "consequentiality" for determining wrongfulness.[125] This test would consider "three dimensions of consequentiality," including "the importance and number of values affected, the extent to which such values are affected, and the number of participants whose values are so affected."[126] Under this approach, he suggests consideration of the scale of an operation, the effects it produces in the target state, and its reach in terms of actors involuntarily affected.[127]

There is merit to Watts's approach, perhaps with slight modification and clarification. First, as is often the case, it presupposes a consummated intervention. For the rule to have any true force and effect, it needs to operate prophylactically—both as a deterrent and potentially as a justification for measures intended to thwart an actual or anticipated intervention before

it works its harm. Responding to an intervention after the fact is suboptimal, because it may be too late at that point to prevent harm. Thus, the consequentiality test, or any other, must consider potential, not actual, harm.[128]

Second, the number of participants whose values are affected is not a particularly helpful dimension. It is just one measure of the extent to which sovereign values are affected and is a highly dependent variable. This is apparent in the case of election interference through covert deception, where the populace, or subsets thereof, are the primary targets of an operation or campaign, and swaying or dissuading votes or generally causing distrust in the results is the aim. In general terms, the degree to which the sovereign value of a free and fair election will be affected will likely be a function of the number of voters deceived. One can imagine how the viral spread of false reports of a candidate's withdrawal from a closely contested race on the eve of an election could swing the results. On the other hand, where such close margins are at play, it might only require a handful of voters to alter the outcome. In either case, the consequence is the same.

Thus, consequentiality, or perhaps better stated, potential impact, is better understood as an assessment of the inverse relationship between the relative value of the targeted interest and the anticipated extent to which the interest will be affected. Even among the bundle of rights falling within the *domaine réservé*, there are necessarily qualitative differences. As evidenced by recent state pronouncements, independence over the choice of a state's political system, that is, election processes and results, is at the core of protected sovereign interests.[129] For heavily weighted interests such as elections, there should be lower tolerance for interventions aimed at undermining their independence. In such cases, there should be a strong presumption that covert deception measures targeting the electorate and election processes constitute a prohibited intervention.

Some states have recently expressed a view that cyber operations intended to disrupt the fundamental operation of legislative bodies or that would destabilize financial systems would violate the nonintervention principle.[130] It is for those states to assign the relative weight of these sovereign interests, and they must bear responsibility for those assessments.

Determining whether a covert disinformation campaign constitutes a prohibited intervention must also account for intent. As noted in the Tallinn Manual 2.0, actions that "have a *de facto* coercive effect must be distinguished from those in which a State intends to coerce *de jure*."[131] While discerning adversary intent is always a challenge, where a campaign of covert deception is involved, intent is perhaps most easily assessed based on the nature of the deception and the target or targets of the covert propaganda being spread. For example, it is apparent from the record that the objective of Russia's disinformation campaign during the last several election cycles was at least to corrupt the process and alter the results. But Russia has not confined its disinformation efforts to disrupting elections. It is also evident from the nature of its deception operations that Russia has engaged in a broader, systematic

campaign to sow division throughout Western democracies, demoralize cultural values, and alter the populations' perceptions of reality. These actions meet almost any definition of subversion, where intent is fairly apparent.[132]

Finally, assessing the potential consequentiality or impact of anticipated or ongoing interference should be done holistically, considering the full context of an action or set of actions and their potential impact on the affected state.[133] Information is but one element of state power and is rarely employed in isolation. For example, analyses that attempt to disaggregate the conglomeration of actions Russia took to impact the 2016 presidential elections ignore context and miss the mark. Russia's actions were synchronized over time and space and mutually supportive—exactly the types of composite acts that "defined in the aggregate" are internationally wrongful.[134]

Conclusion

The advent of the modern, digital information environment has introduced the phenomenon of cyber conflict and fundamentally recast the nature of information conflict. Taking cues from Russia's covert influence efforts, China and other revisionist states are more actively stepping into the information conflict arena, and the United States' national-security apparatus is rightfully taking note. The recognition of this emerging threat is beginning to drive the United States' strategic orientation and efforts to better defend against hostile foreign influence campaigns. International law can and should play a role in these efforts.

The rise of hostile cyber operations and the resurgence and evolution of information conflict have placed renewed emphasis on the principle of nonintervention as a tool for regulating interstate relations in the gray zone below and outside of armed hostilities. This renewed emphasis on the rule has also highlighted its definitional weaknesses—flaws that limit its immediate value as a means for regulating cyber and information conflict and risk, casting it as an anachronism. Effective adaptation of the rule to account for the realities of cyber and information conflict will require states to establish greater clarity on the core concept of coercion and the boundaries between legitimate and illegitimate nonforcible measures of influence and statecraft. This is difficult terrain, but states should start the process by refocusing on the central interest the nonintervention rule is intended to protect—sovereign equality and independence. Drawing a line between covert deception and overt influence is a sound starting point, consistent with general principles of law common to many domestic legal regimes that recognize and regulate deception as a legally cognizable harm in myriad ways.

A cornerstone of the rules-based international order, international law has played an important role in regulating interstate relations and achieving some semblance of stability and security in the post–World War II era—a proposition reflected in the United States' long-standing commitment to the framework of international law and its contribution to the peaceful resolution of disputes. Any US strategy aimed at effectively addressing ICT-enabled national-security threats, including covert influence and deception campaigns,

should include the United States taking a lead on advancing the role of international law and norms development. Drawing more definitive lines with respect to the role of the rule of nonintervention will serve the dual purpose of deterring adversary states from crossing articulated red lines and, where deterrence fails or is ineffective, underpinning the legitimacy of US counter-cyber and counter-influence responses.

ACKNOWLEDGMENTS

Special thanks to Dillon Chepp (Washington College of Law, JD, 2020) and Matthew Kahn (Harvard Law School, JD candidate, 2022) for their excellent research support for this paper.

NOTES

1 Sun Tzu, *The Art of War*, ⁋ 18, Internet Classics Archive (Lionel Giles trans.), http://classics.mit.edu/Tzu/artwar.html (last visited Jul. 14, 2020).

2 E. de Vattel, The Law of Nations or The Principles of Natural Law 131 (James Brown Scott ed., Charles G. Fenwick trans., Carnegie Institute of Washington 1916) (1758).

3 Rand Waltzman, *The Weaponization of Information: The Need for Cognitive Security: Hearing Before the Subcomm. on Cybersec. of the S. Comm. on Armed Services*, 115th Cong. 1 (2017) [hereinafter Waltzman Testimony] (testimony of Rand Waltzman, senior information scientist, RAND Corp.).

4 *Id*. at 2.

5 For purposes of this paper, information conflict refers to the strategic use of information to influence, disrupt, corrupt, or usurp the decisions and actions of an adversary's government, military, private sector, general population, or a combination thereof.

6 *See, e.g.*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 28(b), U.N. Doc. A/70/174 (July 22, 2015) [hereinafter UN GGE Report].

7 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ⁋ 205 (June 27).

8 Jeremy Wright QC MP, *Cyber and International Law in the 21st Century*, GOV.UK (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

9 Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends xii (2019).

10 Dennis Kux, *Soviet Active Measures and Disinformation: Overview and Assessment*, 15 Parameters—J. U.S. Army War C. 19 (1985). By some counts, the Soviets carried out over 10,000 individual disinformation operations during the Cold War. S. Select Comm. on Intelligence, Russian Active Measures Campaigns and Interference, Volume II: Russia's Use of Social Media with Additional Views, S. Rep. No. 116-XX, at 11–12 (2020).

11 *Inside the KGB: An Interview with Maj. Gen. Oleg Kalugin*, CNN (Jan. 1998).

12 Office of the Dir. of Nat'l Intelligence, Assessing Russian Activities and Intentions in Recent US Elections ii (2017) [hereinafter ODNI Report].

13 *Id*. at 2.

14 *Id*. at 1–4.

15 *See id*. at 4.

16 Indictment, United States v. Internet Research Agency, LLC, No. 1:18-cr-00032-DLF (D.D.C. filed Feb. 16, 2018).

17 *Id*. at 5. Specifically, the indictment alleges the defendants obstructed the lawful functions of the Federal Election Commission, the US Department of Justice, and the US Department of State.

18 *Id*. at 4.

19 S. Select Comm. on Intelligence, *supra* note 10, at 11–12.

20 Margaret L. Taylor, *Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe*, Brookings Institution: TechTank (July 31, 2019), https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe.

21 Nancy Cordes et al., *Intel Officials Warned Lawmakers Russia Trying to Interfere in 2020 Election*, CBS News (Feb. 21, 2020, 11:11 AM), https://www.cbsnews.com/news/russian-election-interference-intelligence-officials-warned-lawmakers-2020.

22 James Frater et al., *EU Says Pro-Kremlin Media Trying to Sow 'Panic and Fear' with Coronavirus Disinformation*, CNN (Mar. 18, 2020, 1:13 PM), https://www.cnn.com/2020/03/18/europe/eu-kremlin-disinformation-coronavirus-intl/index.html.

23 Mazarr, *supra* note 9, at 107 (quoting Murong Xuecun, *The New Face of Chinese Propaganda*, N.Y. Times (Dec. 20, 2013), https://www.nytimes.com/2013/12/21/opinion/sunday/murong-the-new-face-of-chinese-propaganda.html).

24 *Id*. at 114 (quoting President Xi Jinping).

25 Julian E. Barnes, Matthew Rosenberg, and Edward Wong, *As Virus Spreads, China and Russia See Openings for Disinformation*, N.Y. Times (Apr. 10, 2020), https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html.

26 Daniel R. Coats, Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence 7 (2019).

27 Office of the President, Cyber Strategy of the United States of America 41 (2018).

28 UN Charter, art. 2, ¶ 1.

29 Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

30 The *jus ad bellum* refers to the body of customary international law that governs the conditions under which states may resort to force and is reflected in the United Nations Charter. *See* UN Charter, art. 2, ¶ 4; *id*. art. 51.

31 1 Lassa Oppenheim, Oppenheim's International Law 428 (Sir Robert Jennings & Sir Arthur Watts eds., 9th ed. 1992).

32 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ⁋ 202 (June 27). Some assert that sovereignty is itself a primary rule of international law. That issue is beyond the scope of this paper.

33 *See, e.g.*, UN GGE Report, *supra* note 6, at ¶ 28(b) ("In their use of ICTs, States must observe, among other principles of international law . . . non-intervention in the internal affairs of other States.").

34 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 317 (Rule 66) cmt. 18 (Michael Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0].

35 *See* Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-intervention*, in Cyberwar: Law and Ethics for Virtual Conflicts 255 (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., 2015) (noting that jurists and commentators "have struggled to identify the precise contours of the principle and to apply those delineations to ever-evolving and increasingly inter-tangled international relations").

36 Oppenheim, *supra* note 31, at 432.

37 Mohamed Helal, *On Coercion in International Law*, 52 N.Y.U. J. Int'l L. & Pol. 1, 55 (2019).

38 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ⁋ 205 (June 27).

39 Tallinn Manual 2.0, *supra* note 34, at 314 (Rule 66) cmt. 6.

40 *Nicaragua*, 1986 I.C.J. Rep. at ¶ 205 (noting that with regard to "the content of the principle of non-intervention—the Court will define only those aspects of the principle which appear to be relevant to the resolution of the dispute").

41 *Id*. at ¶ 201 (noting that its analysis of the principle of nonintervention served only to "enquire whether there is any justification for the activities in question, to be found not in the right of collective self-defence against an armed attack, but in the right to take counter-measures in response to conduct of Nicaragua which is not alleged to constitute an armed attack").

42 *See* Harriet Moynihan, Chatham House, The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention 27 (2019) (noting that the court's discussion of nonintervention should be considered nonprescriptive dicta).

43 Oppenheim, *supra* note 31, at 432.

44 Philip Kunig, *Prohibition of Intervention*, in Max Planck Encyclopedia of Public International Law (2008), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434.

45 *See, e.g.*, *Coercion*, USLegal, https://definitions.uslegal.com/c/coercion/ (last visited Jul. 25, 2020) ("Coercion generally means to impose one's will on another by means of force or threats.").

46 Oppenheim, *supra* note 31, at 430.

47 *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 Tex. L. Rev. 1579, 1588 (2017) (discussing the concept of *domaine réservé*).

48 Moynihan, *supra* note 42, at 34.

49 *See id.*; Oppenheim, *supra* note 31, at 430–31. The Tallinn Manual 2.0 draws a distinction between inherently governmental functions (protected by the purported rule of sovereignty) and the narrower class of protected interests falling within the *domaine réservé* (protected by the rule of nonintervention). *See* Tallinn Manual 2.0, *supra* note 34, at 24 (Rule 4) cmt. 22 ("Usurpation of an inherently governmental function differs from intervention in that the former deals with inherently governmental functions, whereas the latter involves the *domaine réservé*, concepts that overlap to a degree but that are not identical."). The Tallinn Manual 2.0 offers no further explanation to support this schema of distinct sovereign functions, which makes little sense in light of the broad presumptions of independent internal governance that flow from the principle of sovereignty. *See* Moynihan, *supra* note 42, at 34 ("In any event, since the non-intervention principle derives from and is a reflection of the principle of sovereignty, the better view is that there are not two different standards of matters reserved to a state.").

50 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ⁋ 205 (June 27).

51 S.S. "Lotus" (Fr./Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

52 *See, e.g.*, Tallinn Manual 2.0, *supra* note 34, at 315 (Rule 66) cmt. 10.

53 Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 Yale L.J. Online 1, 7 (2017).

54 Ohlin, *supra* note 47, at 1588.

55 Helal, *supra* note 37, at 66–67 ("The *domaine réservé* . . . is not static. Its breadth is ever-changing depending on the extent of the international legal obligations of a state, the growth of international law, and the intrusiveness of international regulatory and adjudicatory bodies.").

56 Moynihan, *supra* note 42, at 34.

57 Int'l Law Comm'n, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 22, U.N. Doc. A/56/10, at 75 (2001).

58 *See* Tallinn Manual 2.0, *supra* note 34, at 314 (Rule 66) cmt. 7.

59 R. J. Vincent, Nonintervention in the International Order 40 (2015).

60 *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ⁋ 205 (June 27).

61 *See, e.g.*, Jacobson v. Massachusetts, 197 U.S. 11 (1905) (upholding as within the general police power the authority of states to enact and enforce compulsory vaccination laws).

62 *Nicaragua*, 1986 I.C.J. Rep. at ¶ 205. These actions would also constitute prohibited uses of force in violation of Article 2(4) of the Charter, triggering the victim state's inherent right of self-defense under the US view of the *jus ad bellum*. *See id*. Some argue that, implicit in the *Nicaragua* judgment's description is the notion that to constitute coercion, the threatened consequence must itself be unlawful.

63 Schmitt, *supra* note 53, at 8; Tallinn Manual 2.0, *supra* note 34, at 318 (Rule 66) cmt. 21 ("Coercion must be distinguished from persuasion, criticism, public diplomacy, [and] propaganda.").

64 Vincent, *supra* note 59, at 15.

65 For a discussion of the origins of the principle of nonintervention, see *id*. at 20–44.

66 *Id*. at 35–37.

67 *See* Helal, *supra* note 37, at 56 (quoting Tomislav Mitrovic, *Non-Intervention in the Internal Affairs of States*, in Principles of International Law Concerning Friendly Relations and Cooperation 224–25 (Milan Šahović ed., 1972)); Watts, *supra* note 35, at 256 ("Twentieth-century commentators observed that non-intervention prohibits only acts that are 'dictatorial' by nature or effect.").

68 *See* Helal, *supra* note 37, at 56.

69 Oppenheim, *supra* note 31, at 432 (emphasis added), 434.

70 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ⁋ 203 (June 27).

71 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, U.N. GAOR 6th Comm., 25th Sess., Supp. No. 28, U.N. Doc. A/8082 (Oct. 24, 1970).

72 *Nicaragua*, 1986 I.C.J. Rep. at ¶ 205.

73 *Id*.

74 *Id*.

75 Moynihan, *supra* note 42, at 34.

76 *See, e.g.*, *id*. at 29 (noting that in the context of nonintervention, coercion bears a different meaning than in normal usage); Watts, *supra* note 35, at 256 ("In this sense, it is likely that the best understanding of non-intervention appreciates a nuanced and particularized notion of coercion.").

77 Maziar Jamnejad and Michael Wood, *The Principle of Non-intervention*, 22 Leiden J. Int'l L. 345, 381 (2009).

78 *See* Ohlin, *supra* note 47, at 1589.

79 *See id*.

80 Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

81 William Edward Hall, A Treatise on International Law 50 (1895).

82 Oppenheim, *supra* note 31, at 430, 432.

83 Tallinn Manual 2.0, *supra* note 34, at 322 (Rule 66) cmt. 29 ("The fact that a coercive cyber operation fails to produce the desired outcome has no bearing on whether [the nonintervention rule] has been breached.").

84 Moynihan, *supra* note 42, at 28 (quoting Jamnejad and Wood, *supra* note 77, at 348).

85 Harriet Moynihan, *The Application of International Law to Cyberspace: Sovereignty and Non-intervention*, Just Security (Dec. 13, 2019), https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention.

86 Moynihan, *supra* note 42, at 30 (internal citations omitted).

87 Moynihan's effective substitution of "pressure and compulsion" for coercion to distinguish between interference and intervention is less helpful. According those terms their common meaning, it is unclear whether she uses them simply as synonyms for coercion or also to include persuasion and influence which, standing alone, risks over-inclusion.

88 Tallinn Manual 2.0, *supra* note 34, at 317 (Rule 66) cmt. 18.

89 Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 Chi. J. Int'l L. 30, 51 (2018).

90 *See, e.g.*, Schmitt, *supra* note 53, at 8; Ohlin, *supra* note 47, at 1579–80.

91 *See* Tallinn Manual 2.0, *supra* note 34, at 168 (Rule 32) cmt. 5.

92 *See* Schmitt, *supra* note 89, at 51 ("The deceptive nature of [Russian] trolling is what distinguishes it from a mere influence operation."); Helal, *supra* note 37, at 115 ("In times of peace, *covert* or *black* IO, IW, or PSYOPs, are unlawful under the prohibition on intervention if these activities are undertaken to interfere with the *domaine réservé* of a state."); Steven J. Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, Just Security (Jan. 12, 2017), https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion.

93 Schmitt, *supra* note 89, at 51; *see also* Ohlin, *supra* note 47, at 1589 ("In order to count as illegal intervention, the structure of the interaction must have the following form: engage in this action; otherwise you will suffer a particular consequence.").

94 *See* Statute of the International Court of Justice, June 26, 1945, Art. 38(1)(c), 59 Stat. 1055, 33 U.N.T.S. 933; *see also* Restatement (Third) of the Foreign Relations Law of the United States § 102(c)(4) (1987) (recognizing general principles as those "common to the major legal systems, even if not incorporated or reflected in customary law or international agreement, [that] may be invoked as supplementary rules of international law where appropriate").

95 *See generally* Int'l L. Comm'n, Second Report on General Principles of Law, U.N. Doc. A/CN.4/741 (2020) (describing the concept and means of identifying general principles of law).

96 Indictment, United States v. Internet Research Agency, LLC, No. 1:18-cr-00032-DLF, at ¶ 2 (D.D.C. filed Feb. 16, 2018). The Department of Justice has since decided to dismiss charges against two of the corporate defendants due to their "ephemeral presence and immunity to just punishment, the risk of exposure of law enforcement's tools and techniques, and the post-indictment change in the proof available at trial." Motion to Dismiss Concord Defendants, United States v. Internet Research Agency, No. 1:18-cr-00032-DLF, at ¶ 9 (D.D.C. filed Mar. 16, 2020).

97 Indictment, United States v. Internet Research Agency, LLC, No. 1:18-cr-00032-DLF, at ¶ 9 (D.D.C. filed Feb. 16, 2018).

98 Hammerschmidt v. United States, 265 U.S. 182, 188 (1924).

99 U.S. Dep't of Justice, Criminal Resource Manual, 18 U.S.C. § 371—Conspiracy to Defraud the United States, https://www.justice.gov/archives/jm/criminal-resource-manual-923-18-usc-371-conspiracy-defraud-us (last updated Jan. 21, 2020) [hereinafter DOJ Criminal Resource Manual, 18 U.S.C. § 371].

100 *See Hammerschmidt*, 265 U.S. at 188.

101 Charles Doyle, Cong. Research Serv., R41223, Federal Conspiracy Law: A Brief Overview 9 (2020). Although the Special Counsel's indictment does not allege that the defendants' actions altered the outcome of the 2016 presidential election, it is sufficient that there was an injury to the integrity of the government. DOJ Criminal Resource Manual, 18 U.S.C. § 371, *supra* note 99.

102 *See* Stuart P. Green, *Deceit and the Classification of Crimes: Federal Rules of Evidence 609(A)(2) and the Origins of Crimen Falsi*, 90 J. Crim. L. & Criminology 1087, 1095–99 (2000).

103 *See id*. at 1093–94.

104 *See, e.g.*, State v. Abdullah, 967 A.2d 469, 476–77 (R.I. 2009); Davis v. State, 910 So. 2d 1228, 1231 (Miss. Ct. App. 2005).

105 People v. Williams, 305 P.3d 1241, 1245 (Cal. 2013) (citing Rex v. Pear, 168 Eng. Rep. 208 (1779)).

106 Reid v. Commonwealth, 781 S.E.2d 373, 375 n.1 (Va. Ct. App. 2016); *see also Williams*, 305 P.3d at 1241; State v. Barbour, 570 S.E.2d 126, 128 (N.C. Ct. App. 2002).

107 *Williams*, 305 P.3d at 1245.

108 *Id*. (quoting People v. Edwards, 236 P. 944, 948 (Cal. Dist. Ct. App. 1925)).

109 Wayne R. LaFave, 2 Subst. Crim. L. § 17.3(c) (3d ed.), Westlaw (last updated Oct. 2019).

110 Model Penal Code § 2.11(3)(d) (Am. Law Inst., Proposed Official Draft 1962); *see* LaFave, *supra* note 109, at § 17.3(c) n.108 (collecting statutes).

111 LaFave, *supra* note 109, at § 17.3(c) n.98, n.99 (collecting statutes).

112 Pub. L. 106–386, 114 Stat. 1464 (2000) (codified as amended in scattered sections of the US Code).

113 22 U.S.C. §§ 7101(b)(13), 7102(11) (2018). The TVPA directly prohibits sex trafficking obtained by force, fraud, or coercion. 18 U.S.C. § 1591 (2018). The TVPA's prohibitions on forced labor, § 1589, and human trafficking to further forced labor, § 1590, extend to involuntary servitude obtained by fraud, *see* Mairi Nunag-Tanedo v. E. Baton Rouge Parish Sch. Bd., 790 F. Supp. 2d 1134, 1144, 1147 (C.D. Cal. 2011) (refusing to dismiss plaintiffs' claims that defendants violated 18 U.S.C. §§ 1589, 1590 where defendants' fraudulent scheme coerced plaintiffs into performing forced labor).

114 *Mairi Nunag-Tanedo*, 760 F. Supp. 2d at 1145.

115 For example, in the United Kingdom, deception or "dishonesty" forms the basis of numerous criminal and civil proscriptions. *See* Ivey v. Genting Casinos [2018] AC 391 (defining dishonesty for purposes of acquisitive crimes). Brazil's public corruption statute similarly identifies fraud or deception as a means of harming government administration. Lei Anticorrupção [Anticorruption Law] (Lei n. 12.846/2013), art. 5 (Braz.). A number of states also recognize deception as a substitute for force or coercion in sex-related crimes. *See, e.g.*, Código Penal [C.P.] [Penal Code], art. 215 (Braz.); R. v. Cuerrier [1998] 2 S.C.R. 371, 374 (Can.); CrimA 5734/10 Kashour v. State of Israel (Jan. 25, 2012) (Isr.); *Crimes Act 1900* (NSW) s61HE(6) (Austl.); Assange v. Swedish Prosecution Authority [2011] EWHC (Admin) 2849 [87–90] (Eng.).

116 *See, e.g.*, Ruth Levush, *Government Responses to Disinformation on Social Media Platforms: Comparative Summary*, Law Library of Cong., https://www.loc.gov/law/help/social-media-disinformation/compsum.php (last updated Mar. 16, 2020); Luis Acosta, *Regulation of Foreign Involvement in Elections: Comparative Summary*, Law Library of Cong., https://www.loc.gov/law/help/elections/foreign-involvement/index.php (last updated Nov. 8, 2019); Samantha Bradshaw et al., NATO Strategic Comms. Ctr. Excellence, Government Responses to Malicious Use of Social Media (2018).

117 *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) div. 92.2(1)(a)-(c) (intentional), 92.3(1)(a)-(c) (reckless) (Austl.); *id*. at 92.2(2), 92.3(2). Additionally, the actor's conduct must be covert or deceptive, or involve a threat to cause serious harm or a demand "with menaces." *Id*. at 92.2(1)(d), 92.3(1)(d).

118 Att'y-Gen.'s Dep't, Foreign Influence Transparency Scheme: Factsheet 2 (2019) (Austl.).

119 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime, art. 3(a), G.A. Res. 55/25, U.N. Doc. A/55/383 (Nov. 15, 2000).

120 For a general discussion of the crime of perfidy in the cyber context, see Colonel Gary P. Corn & Commander Peter Pascucci, *The Law of Armed Conflict Implications of Covered or Concealed Cyber Operations—Perfidy, Ruses, and the Principle of Passive Distinction*, in The Impact of Emerging Technologies on the Law of Armed Conflict (Maj. Ronald T. P. Alcala & Eric Talbot Jensen eds., 2019).

121 Watts, *supra* note 35, at 249.

122 Ohlin, *supra* note 47, at 1593.

123 Tallinn Manual 2.0, *supra* note 34, at 318 (Rule 66) cmt. 19.

124 *Id*. at 319 (Rule 66) cmt. 21.

125 Watts, *supra* note 35, at 257.

126 *Id*.

127 *Id*.

128 This approach undoubtedly raises legitimate challenges with respect to available intelligence and the ability to assess attribution and prejudge the intent, design, or causal connection to a protected aspect of sovereignty, and the likely impact a planned or ongoing influence operation will have. But these are neither unique nor insurmountable obstacles. States routinely face similar intelligence challenges when evaluating adversary activities and considering responses, such as in the *jus ad bellum* context.

129 *See, e.g.*, Letter from the Minister of Foreign Affairs to the President of the House of Representatives, Letter to the Parliament on the International Legal Order in Cyberspace, Appendix at 3 (July 5, 2019) (Neth.); Honorable Paul C. Ney Jr., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference; Wright, *supra* note 8.

130 Wright, *supra* note 8.

131 Tallinn Manual 2.0, *supra* note 34, at 321 (Rule 66) cmt. 27.

132 Some consider subversion a distinct category of intervention. *See* Watts, *supra* note 35, at 255–56.

133 *See* Tallinn Manual 2.0, *supra* note 34, at 319 (Rule 66) cmt. 21 (noting the view of some experts that actions can rise to the level of an intervention based on the context and consequences).

134 *See* Int'l Law Comm'n, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 15, U.N. Doc. A/56/10, at 62 (2001).

26 25 24 23 22 21 20 7 6 5 4 3 2 1

The preferred citation for this publication is Gary P. Corn, *Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2005 (September 18, 2020), available at https://www.lawfareblog.com/covert-deception-strategic-fraud-and-rule-prohibited-intervention.

About the Author

GARY P. CORN

Colonel (ret.) Gary P. Corn is program director and adjunct professor, Tech, Law, and Security Program, Washington College of Law; senior fellow of national security and cybersecurity, R Street Institute; and founder of Jus Novus Consulting. Corn previously served as staff judge advocate for US Cyber Command and as deputy legal counsel to the chairman of the Joint Chiefs of Staff.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION