Low-Intensity Cyber Operations and the Principle of Non-Intervention

Sean Watts*

Contents
1. Introduction
2. Non-Intervention in the International Legal System
   2.1. Customary Status
   2.2. Relationship to Expressions in Treaties
   2.3. *Ius Cogens* Status
   2.4. Terminology
3. The Meaning of ‘Intervention’
   3.1. Coercion
   3.2. Economic Acts
   3.3. Propaganda
   3.4. UN Charter, Article 2(7) Intervention Distinguished
   3.5. Declaration on the Inadmissibility of Intervention
   3.6. Internal or External Affairs
   3.7. *Domaine Réservé*
   3.8. Subversive Intervention
   3.9. UN Charter, Article 2(7) on Internal Matters
   3.10. External Affairs
   3.11. Motive or Intent
4. Justifications
5. Conclusion

1. Introduction

The principle of non-intervention is an important, though poorly understood and implemented aspect of international law. A legal outgrowth of sovereignty and territorial control, non-intervention prohibits States from coercively imposing their will on the internal and external matters of other States. The pressing need for the principle is clear. It would be difficult to imagine a peaceful system of sovereigns that did not include such a norm. However, the level of clarity and compliance connected with the principle has never been equal to its seeming importance in the international system. Considerable ambiguity and regular breach have long accompanied the principle of non-intervention, leading some even to question its status as law.

* Professor of Law, Creighton University School of Law; Reserve Instructor, United States Military Academy at West Point; Senior Fellow, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.
It is difficult to explain precisely why this critical international norm is in such a state. Perhaps its current condition reflects the limits of substantive consensus in a system comprised of legally equal though politically, economically and militarily unequal and diverse sovereigns? Perhaps intervention as a means of exerting international influence is too attractive to definitively proscribe in the fiercely competitive realm of international politics? Or perhaps competing norms and rules have bested intervention in the competition for States’ finite international legal attention span?

Whatever the forces behind the underdeveloped state of the principle of non-intervention and whatever States’ compliance record, non-intervention undoubtedly occupies an identifiable place on the spectrum of internationally wrongful acts. Somewhere between the prohibition on use of force or armed attack, one of, if not the most severe, wrongful acts between States, and the international law prohibition of simple violations of sovereignty, a comparatively less grave form of internationally wrongful acts, one likely finds the prohibition of intervention. Non-intervention seems to lie at a middle ground of international wrongs – not insignificant, but also not supreme among wrongful acts. 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 simple exercise.

Cyber operations, increasingly common both in the communal and routine senses, have emerged as vital mode of interaction between States. When, where and how States conduct themselves in cyberspace now significantly shapes the condition of their international relations. Early investigations of cyber relations between States focused on the possibility and prospect of massive cyber-attacks producing debilitating and destructive consequences. Though certainly feasible, such cyber cataclysms have proved unlikely events. The interconnected, inter-reliant and networked aspects of cyberspace that make cyber-attacks possible simultaneously counsel States against their haphazard use. An attacking State may stand to lose as much or more than it gains from crippling a competitor’s electronic infrastructure. Low-intensity cyber operations, actions taken short of destructive or violent attacks, present a far more likely picture of future State cyber interactions. In addition to being highly feasible and often inexpensive, low-intensity cyber operations offer attractive prospects for anonymity, appear to frustrate attack correlation by targets, and may also reduce the likelihood of provoking severe retaliation. In short, low-intensity cyber operations offer States appealing opportunities to degrade adversaries while avoiding the likely strategic and legal costs of massively destruction cyber-attacks.

How these low-intensity cyber operations fare under international legal analysis is a topic of increasing importance. Whether the low-level impact, relatively small scale effects and de minimus intrusions of low-intensity cyber operations implicate established international legal norms such as the principle of non-intervention

---


138