

# The Globalization of Hybrid Warfare and the Need for Plausible Deniability

**Benedict E. DeDominicis**

 <https://orcid.org/0000-0001-7743-717X>

*Catholic University of Korea, South Korea*

## INTRODUCTION

This chapter analyzes the utilization of social media as part of hybrid warfare's efforts to undermine state security through covert means that can be illegal or criminal. It begins by highlighting the postwar globalization context that encouraged indirect and covert competitive intervention by nuclear powers within the internal politics of target polities. The post-1945 nuclear environment ended the viable application of deadly force as a purposeful policy option for great powers intentionally to select in order to attain their goals regarding each other. They battle indirectly through competitive interference within the political systems of third actors in addition to targeting not only each other, but also their own national public opinion. The aim of this competitive interference is to enable their respective local political clients at the expense of the perceived local clients of the other intervening competitor. The growth of mass public participation intensified nationalist self-determination political sensitivities. It increased local opposition and raised the political costs of overt external interference. Postwar global human rights norms developed to include national self-determination for all. Covert intervention abroad became politically preferable domestically as well to avoid negative domestic political reactions to perceived imperialism. Covert intervention in all forms decreases political resistance and costs to the intervenor. This chapter highlights how the nature of social media content distribution makes propaganda and disinformation distribution very extensive at relatively very low cost. These trends and advantages furthered the stress on covert intervention and the formation of national security bureaucracies for engaging in it. Social media propaganda operations are branded as disinformation because their source is purposefully disguised. Russian state agency Internet-based covert intervention via social media in the 2016 US national elections demonstrated that the US is part of the politically globalizing world that it helped create after 1945. The policy response to these challenges is likely to include strengthening further the intelligence/counterintelligence capabilities of the national security state.

## BACKGROUND

Adamson (2005) argues that due to American-led postwar economic and political globalization, the differentiation between external and internal security threats is increasingly blurred. "[N]ew security strategies of global policing [and] surveillance [...] that emerge in response to this new environment will need to be accompanied by a set of new political strategies" (p. 44). Soviet-American global competition for political influence in the nuclear setting provided the template for what is today labelled hybrid/cyber warfare including security policy responses to it. "The covert aspect of information and propaganda dissemination ... has been of exceptional importance during the Soviet-American cold war" [*sic*] (Cottam

DOI: 10.4018/978-1-5225-9715-5.ch016

& Gallucci, 1978, p. 32). This external intervention, when observed by mobilized local political actors, would more likely be seen in effect as an intolerable violation of national sovereignty. This interference would contribute to intensifying domestic polarization within the target polity. The exacerbation of the perceived threat from the other would thus appear to vindicate the intervention by their respective external patrons in the eyes of each local client. Disinformation as a component of what is frequently called “hybrid warfare” encourages mobilization to meet the perceived threat (Isikoff & Corn, 2018, p. 44). The local competitor and its external backer depict this resistance-themed disinformation against the alleged threat to national sovereignty as in essence local. The external encouragement and support for one side or the other is purposefully disguised, if not concealed (Voss, 2016, p. 40). The multiple facets of elaborate disinformation campaigns may or may not be illegal. E.g. Russian hacking and theft of more than 150,000 emails from personal or Democratic National Committee linked email addresses was illegal. The intensely competitive for-profit US news media’s utilization of these surreptitiously provided emails via Wikileaks, weakening the Hillary Clinton 2016 presidential campaign as Moscow intended, was not. The complexity of the context intentionally obscures the external intervention in the view of local political actors.

The extent to which this resistance to outside intervention within internal politics may be plausibly portrayed as essentially local was limited. Completely masking external involvement engaging many individuals is not feasible. Aside from the exploitation of new Internet media and communication infrastructure technologies, Washington and Moscow displayed this covert policy behavior historically long before 2016 (Renz, 2016, Ransom, 1977). Target polities included domestic public opinion in addition to foreign publics (Wilford, 2017). Today, so-called hybrid warfare combines national security organizational resource deployments along with exploiting Internet-based technologies to affect the target polity’s power capabilities (Cottam & Gallucci, 1978). The latter include covert psychological social media-oriented public opinion campaigns and damaging Internet-based infrastructure hacking attacks to achieve national security and foreign policy objectives.

Self-determination concomitantly has developed into a human right, although one controversially delineated (Cassese, 2005, pp. 16, 39, 63, 75, 84, 207). Foreign meddling in a targeted polity’s internal political concerns is likely to be condemned by at least some attentive constituencies in the target polity as a desecration of this national community birthright. Determining whether or not it is actually illegal and criminal prevention and punishment is enforceable depends upon the specific legal and political conditions within the target polity. Social media and the Internet in general have expedited this intervention. They have also provided greater opportunities to obfuscate the architect of this interference.

Concurrently, one’s own unofficial collaboration with foreign actors is likely to be self-servingly viewed as not being seditious. The alliance may be formal, i.e. overtly or covertly with intent to receive funds and other material support from a foreign actor. The association may be implicit, such as benefiting from foreign-subsidized social media disinformation operations which were not directly entreated by the local client, but the latter is aware of the intervention. Since the outlay of support was not in the form of a direct disbursement to the local client or other direct donation, it may be more easily categorized as inconsequential. Certain Western political figures and their constituencies view Putin’s regime in Russia as a stronghold for traditional, so-called Christian, conservative family and national values. Post-Soviet era informal collaboration by American partisan competitors with Putin’s regime is therefore less prone to be regarded as potentially treasonous. Rather, it is another alternative resource to oppose the potentially treasonous assimilationist cosmopolitanism that so-called globalist values and their transnational and local collaborator constituencies advocate. According to this conservative populist nationalist worldview, these cosmopolitans are allegedly a threat to the nation’s sovereignty and thus ultimately to the nation’s very existence.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/the-globalization-of-hybrid-warfare-and-the-need-for-plausible-deniability/248045](http://www.igi-global.com/chapter/the-globalization-of-hybrid-warfare-and-the-need-for-plausible-deniability/248045)

## Related Content

---

### Criminological Treatment of Abusing Partners

Guido Travaini, Palmina Caruso, Enrica Beringheli and Isabella Merzagora (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention* (pp. 329-344).

[www.irma-international.org/chapter/criminological-treatment-of-abusing-partners/301158](http://www.irma-international.org/chapter/criminological-treatment-of-abusing-partners/301158)

### Psychology Applied to Prevention and Detection of Human Trafficking

Laura Dryjanska (2022). *Paths to the Prevention and Detection of Human Trafficking* (pp. 44-63).

[www.irma-international.org/chapter/psychology-applied-to-prevention-and-detection-of-human-trafficking/304610](http://www.irma-international.org/chapter/psychology-applied-to-prevention-and-detection-of-human-trafficking/304610)

### Privacy, Ethics, and the Dark Web

Richard T. Herschel (2020). *Encyclopedia of Criminal Activities and the Deep Web* (pp. 140-151).

[www.irma-international.org/chapter/privacy-ethics-and-the-dark-web/248037](http://www.irma-international.org/chapter/privacy-ethics-and-the-dark-web/248037)

### Homophobic Conduct as Normative Masculinity Test: Victimization, Male Hierarchies, and Heterosexualizing Violence in Hate Crimes

Cirus Rinaldi (2020). *Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support* (pp. 100-123).

[www.irma-international.org/chapter/homophobic-conduct-as-normative-masculinity-test/241467](http://www.irma-international.org/chapter/homophobic-conduct-as-normative-masculinity-test/241467)

### Modus Operandi in Cybercrime

Bettina Pospisil, Edith Huber, Gerald Quirchmayr and Walter Seboeck (2020). *Encyclopedia of Criminal Activities and the Deep Web* (pp. 193-209).

[www.irma-international.org/chapter/modus-operandi-in-cybercrime/248041](http://www.irma-international.org/chapter/modus-operandi-in-cybercrime/248041)