“PSYOPS”, State-sponsored online disinformation in international law

Letrone William, Axel

(Degree)
博士（法学）
(Date of Degree)
2023-03-25
(Date of Publication)
2025-03-25
(Resource Type)
doctoral thesis
(Report Number)
甲第8673号
(URL)
https://hdl.handle.net/20.500.14094/0100482421

Summary of the Doctoral Dissertation

Name: LETRONE WILLIAM AXEL

Department: International Cooperation Policy Studies

Title of Dissertation (In case of foreign language, translation into Japanese is required.) “PSYOPS”, State-sponsored online disinformation in international law (“PSYOPS”, 国 家が関与するサイバー空間での情報操作：国際法の観点から)

Summary of Dissertation

"Psychological warfare", as the act of manipulating the information to change the mind of a predetermined target for strategic purposes, is now undergoing a major evolution: it is becoming "cyber-enabled." This is an opportunity to revisit the international law applicable to international communications and to elaborate under-developed areas of international law.

Since the advent of cyberspace, information power, or the capacity to influence behaviours through the manipulation, control or denial of information has become an indissociable aspect of state's national power. Meanwhile, interstate competition unfolds online as it does in the real world. States have learned to leverage information power to influence foreign populations with the aim of gaining strategic advantages. They have done so, notably, through conducting psychological operations online (hereinafter PSYOPS).

There are acceptable and unacceptable PSYOPS. Public diplomacy, unobtrusive and overt communications campaigns intended to promote a policy or an ideology in good faith may be considered acceptable PSYOPS. In contrast, disinformation campaigns, as coordinated releases of false, misleading or harmful information to induce negative feelings among the audience constitute unacceptable PSYOPS.

Unfortunately, states are not always using their information power the right way. Some were accused of sponsoring online disinformation activities to interfere in foreign democratic elections, other were accused of turning a blind eye on disinformation industries operating from within their respective territories. Yet, despite a noticeable surge of attention for online disinformation and the threat the phenomenon represents for democratic institutions around the world, the safety of individuals, and international peace in general, it remains unclear whether any of the accused has breached the law. This state of affairs is both unsurprising and frustrating. Indeed, one the one hand, psychological warfare has always existed. The question of the regulation of subversive, bellicose and defamatory propaganda, including disinformation campaigns, was already an important topic during the Cold War. However, whether by lack of commitment from the part of states, or because abuses of law would have been difficult to avoid in the context of international communications, regulations were kept at a minimum. On the other hand, today cyberspace provides a new interconnected space where states and non-state actors can reach and manipulate audiences of unprecedented size while still maintaining plausible deniability. This new paradigm is highly conducive to information misuses. Therefore, in a context where truth and authentic information have never been so essential to the well-

functioning of our modern information societies, and where "the homeland is no longer a sanctuary"[1], the question inevitably arises as to whether international law provides appropriate protection to the legitimate interests of individuals and states when these are threatened by foreign PSYOPS.

Thus, this work is a study of the international law applicable to PSYOPS, with a focus on online disinformation. It gives an overview of the relevant laws and identifies salient points in the law that should require more consideration. Overall, this work is based on two general ideas; First, the current legal framework for the conduct of psychological warfare perpetuates impunity for information misuse. There is a need to clarify the law in light of new and foreseeable developments in the domain of information and communication technologies. Second, despite their relevance to the subject at hand, too little attention is given to human rights and the correlative due diligence duties of prevention when it comes to regulate state-sponsored disinformation campaigns. And yet, international human rights law contains particularly interesting tools for setting adequate boundaries to psychological warfare and preventing information misuses that can have dramatic consequences on the rights of the audience.

This work is divided into five chapters. The first two chapters set the stage for the legal assessments. The first chapter focusses on defining disinformation. It does so, by commenting on the defining features of the phenomenon, by comparing disinformation with the different types of propaganda, and by highlighting the difficulties commonly associated with analysing disinformation campaigns, such as the questions of intent and causality.

The second chapter takes a historical approach to the question of the regulation of international communication. It is shown that, while pre-cyber propaganda activities may contain disinformation aspects, the phenomenon as it is currently understood by states and practitioners mostly escapes straight-forwards legal characterizations. The dearth of official statements referring to the legal status of foreign disinformation campaigns shows that, the same way as espionage activities, PSYOPS in general, and disinformation campaigns in particular, belong to the grey areas of international law. In other words, state-sponsored PSYOPS,

[1] Lt. Gen. Lori Reynolds in Andrew Milburn & Shawna Sinnott, "Competing for Influence: Operations in the Information Environment" (16 January 2021), Modern War Institute Irregular Affairs podcast, <https://mwi.usma.edu/competing-for-influence-operations-in-the-information-environment/>.

including disinformation campaigns, are presumed lawful until proven otherwise. But when exactly would state-sponsored disinformation campaigns breach international law? The next chapters provide an answer to this question.

A third chapter looks at state-sponsored disinformation activities through the lenses of relevant international rules, principles and treaties safeguarding the interests of states against the behaviours of foreign actors. In doing so, it elicits the circumstances under which a foreign disinformation campaign could exceed the boundaries set by said rules. It is first shown that the 1936 Broadcasting Convention and the 1953 Correction Convention, albeit interesting in their approach to international communications, are difficult to operationalize in presence of covert, cyber-enabled activities. The assessment then turns to the customary principles of the non-use and threat of force and non-intervention. It is explained that these principles could find an application to the context of foreign disinformation activities in very limited circumstances. Note is for example taken of the contemporary debate pertaining to the need to re-interpret the non-intervention principle. It is however cautioned against tinkering the rules for the sole purpose of encompassing more modern forms of PSYOPS, as doing so risks rendering them meaningless, making them prone to instrumentalization by states.

The fourth chapter focusses on human rights law. In covering the relevant rights, the chapter delineates the scopes of the freedom of thoughts and opinion, the right to internal self-determination and the right to life. It is thus shown that state-sponsored disinformation also infringes fundamental human rights. In fact, human right law seems the better approach to state-sponsored disinformation. More specifically, is it noted that each one of the covered right could compensate for the *lacunae* of the aforementioned state-centric rules without entailing excessive risks of instrumentalization by states. The chapter concludes by suggesting an interpretation of human rights extraterritoriality that could give effectivity to the framework thus defined.

The fifth and last chapter deals with the question of attribution and negligence. Notably, it is shown that classic attribution regimes may not provide an adequate path for the attribution of disinformation campaigns to a state, even when a connivence between a state and the private actors involved in the spread of disinformation is obvious. The means of responses in case of successful attribution remain extremely limited anyway. As a solution, it is suggested to look at state accountability from the perspective of the positive duties held by states with respect to the prevention of transboundary international law violations arising from activities perpetrated by private actors in their territories. In other words, information misuses should be looked at through the lenses of due diligence. Due diligence obligations must first be grounded in the law in order to exist. That is to say, duties of due diligence with respect to disinformation arise only if it is attested that disinformation campaigns are susceptible of breaching the law. On this point, this work shows that PSYOPS including disinformation may impair fundamental human rights, and even, in rare occasions, infringe on the rights of states. Hence, it is argued that a state of emission should incur liability for transboundary international law violations, including violations of human rights, arising from disinformation activities conducted by non-state actors operating from within its territory, or under its control, if it is apparent that said state was negligent in preventing information misuses it was entitled and in capacity to act upon. Additionally, it is recalled that under the consensual principle of territorial jurisdiction, recipient states are bound by obligations of prevention of human rights violations *vis à vis* their own population. This translates, in the disinformation context, in various due diligence duties to ensure that the collective will is protected against undue attempts to corrupt the authenticity of democratic processes in times of democratic elections, that adequate laws are in place to regulate egregious speeches, and, most importantly, that independent fact checking networks are not repressed and that sufficient resources are devoted to the development of information literacy. One may also think about an obligation of the receiving state to ensure that the largest service providers are diligent in preventing human right violation arising from information misuses in their platforms.

The burden of prevention should be shared between states and digital platforms, as the latter's services enable psychological warfare. Thus, key social media platform owners should implement corporate due diligence duties in the context of their activities. Of course, even non-state actors would be required to act diligently in prevention abuses arising from information misuses. This means, above all, that the platforms' own prevention efforts are not done to the detriment of the rights of the users. Therefore, social media platforms should devote more attention to designing recommender systems that are less manipulative and less prone to instrumentalization by an external actor. With that being said, corporate due diligence should not deviate attention from improving state accountability in the disinformation context.

(Name: LETRONE WILLIAM AXEL No. 6)

Too often psychological warfare is conducted in complete disregard for human rights. Thus, not only is it time to consolidate human rights in light of users' ever-growing vulnerability, but opening the possibility of engaging the responsibility of states and platforms for blatant negligence in dealing properly with disinformation campaigns seems a promising way forwards.

Name of Academic Advisor: Professor Hayashi Mika