The Hague Centre for Strategic Studies

HCSS PAPER SERIES – CASE STUDY 2

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 2: Responding to Russian Disinformation in Peacetime

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

From Blurred Lines to Red Lines
How Countermeasures and Norms Shape Hybrid Conflict

HCSS Progress
The Hague Centre for Strategic Studies

This case study is part of a five-part paper series, which is compiled into the full report "From Blurred Lines to Red Lines - How Countermeasures and Norms Shape Hybrid Conflict".

Full Report Authors: Louk Faesen, Tim Sweijs, Alexander Klimburg, Conor MacNamara and Michael Mazarr
Reviewers: Pieter Bindt, Frank Bekkers and Richard Ghiasy
September 2020

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Design: Mihai Eduard Coliban (layout) and Constantin Nimigean (typesetting).

The Hague Centre for Strategic Studies
info@hcss.nl
hcss.nl

Lange Voorhout 1
2514EA
The Hague
The Netherlands

HCSS PAPER SERIES | CASE STUDY 2

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 2: Responding to Russian Disinformation in Peacetime

Table of contents

About the Paper Series

This paper is part of the paper series "From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict". The series analyzes effective responses against hybrid threats by evaluating the ways in which countermeasures and norms can help shape appropriate state behavior in the hybrid realm. The series unpacks the logic driving norm development across five different cases, yielding a better understanding of the norm strategies, tools of influence, dilemmas and trade-offs by European states and the US in their response to adversarial hybrid operations, including cyber operations (Russia); disinformation (Russia); propaganda (ISIS); economic espionage (China); maritime claims (China) (see Table 1). The starting point of each case is the hybrid offensive campaign, followed by a description of the western countermeasures and their underlying legal or doctrinal mandate. The normative dimension of each case assesses whether and how the countermeasures reaffirm or establish new norms, and finally identifies their second-order normative effects that are too often ignored and risk undermining the initiator's long-term strategic goals. The case studies are published individually as a paper series and compiled in a full report with complete overview of the theoretical underpinnings of norm development and the key insights that emerge from the analysis, as well as the concluding remarks and policy recommendations.

Paper Series | From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 1
Protecting Electoral Infrastructure from Russian cyberoperations

Case Study 2
Responding to Russian disinformation in peacetime

Case Study 3
Countering ISIS propaganda in conflict theatres

Case Study 4
Responding to Chinese economic espionage

Case Study 5
Upholding Freedom of Navigation in the South China Sea

Read the full report here.

	Case	Countermeasures	Second-Order Normative Effects	Norms
1	**Protecting Electoral Infrastructure from Russian cyberoperations**	Detailed public attribution	Higher burden of proof	***Norm emergence*** prohibiting cyberoperations against electoral infrastructure
		Indictments	Lawfare escalation	
		Sanctions	n/a	
		Diplomatic expulsion	n/a	
2	**Responding to Russian disinformation in peacetime**	Resilience	n/a	***Norm proposal*** against disinformation as covert election interference based on noninterference
		Discrediting media as propaganda	Politicians labeling media as propaganda	
		Overt offensive cyber operation	Weaponization of information	
		Cyber pre-deployment in critical infrastructure	Norm of mutual hostage-taking	
3	**Countering ISIS propaganda in conflict theatres**	Strategic communication	Success of wartime offensive cyber operations over STRATCOM informed U.S. response to similar threats in peacetime.	***Norm proposal*** truthfulness as a benchmark for information operations
		Psychologic operations		
		Covert offensive cyber operation		
4	**Responding to Chinese economic espionage**	Sanctions	Tariff war reduces Chinese incentives for norm adherence and isolates norm violation as bilateral issue	***Norm emergence*** prohibiting cyber-enabled IP theft for economic benefits
		Indictments	Lawfare escalation	
		Bilateral agreement predicated upon improved relations	Souring of bilateral relations reduced Chinese incentives for adherence	
5	**Upholding Freedom of Navigation in the South China Sea**	Arbitration / legal challenge	Political unwillingness to enforce legal ruling	***Norm contestation or revision*** of previously internalized UNCLOS norm of freedom of navigation
		Freedom of Navigation Operations (FONOPs)	Potential of unintended escalation	
		Diplomatic Engagement	n/a	

Table 1: Five case studies of hybrid campaigns, countermeasures and norms promotion

2

Responding to Russian Disinformation in Peacetime

Between 2016 and 2018, Russia conducted disinformation campaigns targeting the U.S. presidential and mid-term elections, and the French presidential election.

Countermeasures

Resilience: The Macron campaign used tested information security measures to pre-empt, delay, discredit and minimize the effects of Russian disinformation

Discredit Media as Propaganda: The Macron campaign disaccredited Russian media outlets Russia Today and Sputnik as propaganda and threatened legal action.

Offensive Cyber Operations: The U.S. embarked on an offensive cyber operation against the Russian troll factory "the Internet Research Agency", effectively shutting it down for several days.

Cyber Pre-Deployment: The U.S. pre-deployed malware within Russia's critical infrastructure. This amounted to a means of coercive signaling to deter further Russian interference.

Second-order normative effects

The second order-normative effects of resilience measures were not considered in this case.

This may set the precedent for other political actors to employ similar measures against legitimate journalists on the same basis.

In responding with offensive cyber effects, the U.S. implied that it is now acceptable to hack what one considers 'fake news', and that it perceives and weaponizes information in the same way as Russia.

While U.S. actions did not violate the UN norm prohibiting cyber operations against critical infrastructure, these actions still implied that the U.S. has implicitly accepted a norm of mutual hostage taking in cyberspace.

Norm proposal

A norm against disinformation as covert election interference

If entrepreneurs would pursue such a norm proposal, it can be *framed* to covert election interference and *linked* to the non-intervention principle. Doing so would prohibit covert influence operations aimed at undermining democratic processes, while still allowing the West to overtly promote democratic principles abroad.

1. Introduction

Conflicts between states are taking on new forms. Russian and Chinese hybrid activities are intended to circumvent detection, existing norms and laws, and response thresholds. They minimize the basis for decisive responses and have introduced a new model of conflict fought by proxy, across domains, and below the conventional war threshold to advance a country's foreign policy goals. A particular challenge associated with this form of conflict is that in some cases there is a lack of explicit norms or rules, while in others it is unclear when and, more specifically, *how* existing international law and norms are to be interpreted and applied in such a context. Against this backdrop, there is significant concern that the ability of Western governments to successfully manage the threat of a major hybrid conflict is hampered by difficulties in attribution, timely response, and escalation control. Yet there are instruments of statecraft available to the defender to level the playing field and shape adversarial conflict behavior. One such tool, in many ways the foundation for all others, is the active cultivation of international norms to shape adversarial hybrid conflict behavior. This paper series evaluates the strategic utility of such norms and considers how countermeasures can be instrumental in establishing and upholding such norms.

This paper analyzes the diplomatic and military countermeasures by the U.S. and French governments in response to Russian information warfare campaigns in 2016 and 2018 as part of their larger hybrid campaign aimed at undermining democratic institutions and processes. More specifically, the paper takes a closer look at the underlying mandate of the countermeasures, their second-order normative effects, and whether they reaffirmed existing norms or established new norms.

The French and American countermeasures were aimed at derailing or delegitimizing Russian disinformation by denouncing and breaking a pattern of behavior that could otherwise establish a norm. As of now, disinformation on its own is not explicitly illegal according to international law, nor is there a norm that emerged specifically dedicated to it. In lieu of explicit norm emergence, our analysis offers suggestions for *framing* and *linking* a norm proposal against disinformation, as well as first steps to assist in socialization. *Framing* it around covert election interference and *linking* to the nonintervention principle would prohibit concerted Russian covert influence operations aimed at undermining democratic processes, while allowing overt support for democratic processes and voices. The suggested norm would form a compromise of sorts: overt means of any sort, including 'propaganda' by state media actors such as

RT (or from a Russian point of view BBC or CNN) would be considered acceptable, as would however publicly declared funding of civil society organizations (such as the U.S. National Endowment of Democracy or the Russian Russkiy Mir Foundation. Starting with a unilateral ban on covert election inteference, facilitated by linking the norm to national security interests, would not only allow a first-mover advantage in framing the issue but would also combat the perception that liberal democracies conduct to covert influencing activity. Afterwards, the entrepreneur should use a coalition or alliance as an organizational platform to socialize the norm with partners and lay the groundwork for opening discussions with Russia on its elections interference, and to sanction countries that continue to covertly interfere in elections. It can adopt a similar strategy as with the Chinese IP theft norm, where the United States and allies would need to agree to abstain from covert election interference even if they are already not doing so in order to allow the Russian government sufficient cover to present any agreement to its citizens as a triumph for Russia. This is obviously just one approach that need not frame a 'final norm' to the overarching problem of disinformation. But it may form a beginning.

The paper is structured as follows: Chapter 2 offers a summary of the theory around norms, including the norm lifecycle and tools of influence to push for norm cascade and internalization. Chapter 3 applies the theoretical framework to the case study and identifies key findings concerning the promotion of international norms that emerged from the analysis. Chapter 4 offers the recommendations from the *entire paper series* on how to promote international norms in the hybrid realm.

2. Norms Primer

The utility of norms and their processes in the hybrid context derives from their dynamic character, making them a more flexible and faster alternative than binding law to manage emerging threats, even as they remain difficult to enforce due to their voluntary nature. Despite deviations in adherence by some actors, norms remain an important tool to establish predictability and signal interstate consensus on what constitutes bad behavior – a yardstick which the international community can leverage when calling out unscrupulous states.[1] The propagation of norms in the realm of hybrid conflict is therefore an important instrument in shaping hybrid threat actors. By identifying the levers of influence and strategic choices that norm entrepreneurs need to take into context, norm ingredients, the tools of influence and their potential trade-offs, they become more aware of their strategies for norm development. Ultimately, the success of a norm rests not just in its content, but in its process: who pushes it, accepts it, and where, when, and how they do so.[2] This section summarizes these components as part of the norm lifecycle to allow for a structured and enhanced understanding of norm development in the hybrid realm. A detailed description of the theory behind norm development is provided in the full report. The lifecycle will function as the theoretical underpinning that informs how norms emerge and eventually are accepted and internalized in the hybrid realm, thereby guiding our own assessment of malicious state activity, but also the normative nature and range of our own response to hybrid threats.

2.1 What is a Norm?

A norm is broadly defined as "a collective expectation for the proper behavior of actors with a given identity", consisting of the four core elements: identity, propriety, behavior and collective expectation (see Table 2).[3] That is, they are voluntary standards for agreeing what constitutes responsible behavior. Because of their voluntary

1 Chertoff, Michael; Reddy, Latha; Klimburg, Alexander, "Facing the Cyber Pandemic", Project Syndicate (11 June, 2020): https://www.project-syndicate.org/commentary/pandemic-cybercrime-demands-new-public-core-norm-by-michael-chertoff-et-al-2020-06.

2 Finnemore, Martha; Sikkink, Kathryn: "International Norm Dynamics and Political Change", International Organizations 52, no. 4 (1998): https://www.jstor.org/stable/2601361?seq=1.

3 Katzenstein, Peter J., "The Culture of National Security: Norms and Identity in World Politics", Columbia University Press (1996).

nature, reaching agreement on more broadly defined norms circumvents lengthy and contentious legal issues while keeping interstate channels of communication open.

Identity (the *who*) refers to the entrepreneur and the target audience. The group targeted by the norm will be affected depending on the norm's framing and linking to a context - military, law-enforcement, economic. The entrepreneur may decide to push the norm bilaterally, multilaterally, or globally, each with its own set of advantages and disadvantages. Overall, the smaller and more identical the pairing, the lower the transaction costs are to obtain information about each side's interests and values.	***Propriety*** (the *how*) is the ideational basis upon which norms make their claim. Norm entrepreneurs should be aware of the trade-offs in pursuing norms with law/treaties (binding) and politics (non-binding) as a proprietary basis. Treaties are state-led, offer harder assurances for internalization through ratification, require significant resources, and are harder to change. Political commitments are an agile and faster alternative that comes with fewer terminological disagreements and is not limited to states.
Behavior (the *what* and *where*) denotes the actions required by the norm of the community. Entrepreneurs establish norms anchored within their social construction of reality to advance their own interests and values. Behavior therefore not only asks what the norm says but also where it resides. Grafting a norm to an organizational platform means grafting it to the culture of an institution, thereby shaping its content.	***Collective expectations*** (the *why*) underpin the social and intersubjective character of the social construction of norms. Entrepreneurs should be aware that others may agree to the norm for different reasons and use this to their advantage. Incompletely theorized norms – where actors disagree as to why the norm exists – and insincere commitments can eventually lead to norm internalization.

Table 2: Four core ingredients of a norm: identity, propriety, behavior, and collective expectations.

The pluralistic nature of norms indicates that a norm entrepreneur has multiple identities and is part of multiple organizational platforms or institutions that may work in tandem coherently and harmoniously but may also conflict in certain contexts.[4] The entrepreneur may then need to prioritize one of them. Norm processes are thus complicated by the uncertainty of which identity, and which underlying norms, the entrepreneur is perceived to prioritize in a particular situation.

Norms and interests are closely related to each other: the former should be seen as generative of, and complementary to, interests pursued by agents rather than as opposed to them.[5] Part of a norm's utility in the hybrid realm, and conversely part of its limitation, is its dynamic nature. There is no set process for norm adaptation

4 Finnemore, Martha; Hollis, Duncan, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity", European Journal of International Law (2020), p. 455: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347958.

5 Keohane, Robert, "Social Norms and Agency in World Politics", NYU School of Law (2010): http://www.law.nyu.edu/sites/default/files/siwp/Keohane.pdf.

and internalization, even if the macro processes for how they operate are generally understood. Norms are not fixed products of agreements, nor are they static nodes of international relations. The accumulation of shared understanding gives norms depth and makes them more robust.

2.2 The Norm Lifecycle

How do norms emerge? Finnemore and Sikkink's model of the norm lifecycle allows for a structured and enhanced understanding of norm development and propagation.[6] The norm lifecycle catalogs the development and propagation of norms across three stages: norm emergence, norm cascade and norm internalization (see Table 3):

Stage 1: Norm Emergence	Stage 2: Norm Cascade	Stage 3: Norm Internalization
Habit and repetition alone – particularly when they go unchallenged – create norms. Alternatively, it can be a dedicated effort by a norm entrepreneur, who has the first-mover advantage of *framing* a norm within a preferential context and *linking* it to other pre-existing norms, which not only increases its credibility and urgency but also anchors the norm within the values and interests of the entrepreneur.	Once a sufficient number of actors have been persuaded by the entrepreneur or even coerced into acceptance, it can trigger socialization effects, like bandwagoning or mimicry, on the remaining hold-outs, accelerating the norm towards widespread acceptance. This process is accelerated when the norm is grafted to organizational platforms.	When a norm is internalized it is 'taken for granted' and no longer considered 'good behavior'; rather it becomes a foundational expectation of acceptable behavior by the international community. Once internalized, a norm shapes the interests of states rather than vice versa. Internalized norms however continue to evolve as the interests, context, identity, and propriety change around them.

Table 3: The three stages of the norm lifecycle: Norm emergence, norm cascade, norm internalization

Habit and repetition alone – particularly when they go unchallenged – create norms.[7] This does not only apply to the hybrid threat actor – for example China normalizing IP theft – but also to the victim undertaking countermeasures that denounce and break a pattern of behavior to keep the hybrid actor from establishing new norms. The victim's countermeasures may itself establish new norms or have second-order normative effects. Regulatory norms known to reside in the diplomatic processes as an alternative

6 Finnemore, Martha; Sikkink, Kathryn: "International Norm Dynamics and Political Change", International Organizations 52, no. 4 (1998): https://www.jstor.org/stable/2601361?seq=1.

7 Sugden, Robert, "Spontaneous Order", Journal of Economic Perspectives 85, no. 4, (1989), pp.87-97: http://www.jstor.org/stable/1942911.

to international law, however, do not emerge spontaneously out of habit. They are the result of dedicated work by actors to promote a new standard of behavior for reasons ranging from self-interest and values to ideational commitment. These actors are the norm entrepreneurs that may be any group of actors. Given our focus on interstate hybrid conflict, we primarily focus on states as norm entrepreneurs. Their efforts are shaped and constrained by existing context and understandings, in that the norm they propose operates alongside pre-existing norms within or outside of their regime complex, without clear hierarchies or processes for resolving overlap, conflict, or coherence.[8]

2.3 Tools of Influence

Once a norm has emerged and gathered a base level of support, two processes that take place simultaneously can contribute to the development of the norm: the norm cascades into widespread adoption (broad acceptance) and reaches internalization (deep acceptance). In promoting norms, norm entrepreneurs can make use of three tools of influence: socialization, persuasion and coercion (see Table 4).[9] The tools of influence that contribute to cascade and internalization come with their own set of costs and benefits on the basis of which entrepreneurs must continuously (re)evaluate their choice based on their interests and the changing context.

Socialization leverages the shared relations and identities between actors and institutions, in order to push a norm towards conformity. It includes forms of mimicry or conformity based on national interests, such as rationally expressive action, social camouflage, bandwagoning, insincere commitments to avoid stigmatization, or improved relations.	***Persuasion*** can occur through cognitive means (through *linking* or *framing*) or material incentives. Persuading actors with very different values and interest systems is difficult unless the norm is incompletely theorized. Persuading actors through ***incentives,*** such as trade agreements, is mostly a tool available to strong states as they require a vast amount of resources over a longer period of time.	***Coercion*** refers to the use of negative inducements, such as sanctions, threats, and indictments to promote the norms of the strong. It mostly remains a tool for strong states who have attribution capabilities and political will. When entrepreneurs face opposition from other actors, incentives and coercion can play a large role at the contentious stages of the norm lifecycle – where contestation is high.

Table 4 Three strategies for norm promotion: socialization, persuasion, coercion.

8 Klimburg, Alexander, and Louk Faesen. "A Balance of Power in Cyberspace." In "Governing Cyberspace - Behavior, Power, and Diplomacy", Rowman & Littlefield, pp. 145–73. (2020): https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf.

9 Finnemore, Martha; Hollis, Duncan, "Constructing Norms for Global Cybersecurity." The American Journal of International Law 110: (2016), pp. 425–479.

While states may initially adhere to norms not because of their content but as part of tactical bargains that serve their interests, in response to incentives or coercion, norm internalization or compliance may still become routinized as habits take hold, such that norm-conforming behavior continues even after the incentives.[10] Over time, tactical concessions, perceived as insincere, may therefore still lead to norm internalization. An entrepreneur should take advantage of the wider spectrum of tools and realize where they enforce their strategy or potentially crowd out other tools.

10 Finnemore and Hollis, "Constructing Norms for Global Cybersecurity.", 425–479.

3. Case Study: Responding to Russian Disinformation in Peacetime

The norm lifecycle provides the theoretical basis through which we can now analyze norm development in a case study to better understand the real-life strategies, tools of influence, dilemmas, and trade-offs that empower state-led norm processes. The dynamics between countermeasures and norms are analyzed as part of the strategies adopted by the U.S. and France toward Russian disinformation, as part of its larger information warfare campaign aimed at undermining democratic institutions and processes, and how they may lead to *framing* and *linking* a norm proposal against disinformation, as well as first steps to assist in socialization

The normative dimension of this case is analyzed at different levels. First, as previously described, states are aware that habit and repetition alone – especially when they go unchallenged – create norms. The Western countermeasures were aimed at derailing or delegitimizing unwanted Russian behavior from establishing new norms. Second, we assess whether the countermeasures reaffirm existing norms or whether they lead to the emergence of a new norm that shapes the behavior of the opponent. Third, if a new norm emerges, we assess its position within the norm lifecycle and identify the tools of influence used for cultivation. Finally, as states pursue what they may perceive as norm-enforcing behavior, their countermeasures may trigger second-order effects. These effects are often underestimated or even ignored when states consider their countermeasures, even though they may produce unintended negative outcomes that risk undermining the initiator's long-term strategic goals. It is important to view these consequences in the context of their impact upon the long-term stability of established norms, focusing on how they set new precedents or affects the socialization that keeps otherwise non-abiding actors in adherence to the overall normative status quo.

Prior to the normative analysis, a description is given of the Russian hybrid operation, followed by the Western countermeasures and their underlying mandate. Herein, we use a broader interpretation of countermeasures than the strictly legal definition. Countermeasures encompass the broad range of State responses taken horizontally both across the Diplomatic, Information, Military, Economic, and Legal (DIMEL) spectrum and vertically in the context of an escalation ladder through which the victim tries to shape the behavior of the opponent, deny benefits and impose costs.

These responses can be cataloged along a spectrum of preventive action to thwart an anticipated threat to reactive responses, which denote pre- and post-attack defensive actions.[11] Throughout the case studies, we predominantly focus on reactive measures and give a cursory glance at the preventive measures when considering how the reactive measures fit into the broader response posture of the state.

Structure of the case study:

a) **Incident**: a description of the hybrid offense.
b) **Countermeasures**: a description of the countermeasures taken by the victim, and their underlying legal or doctrinal mandates.
c) **Normative Dimension:** an analysis of the norm that emerges from the countermeasure.
   i. Norms: do the countermeasures reaffirm existing norms, or do they establish a new norm?
   ii. Application of the norm lifecycle to the norm: what tools of influence are used to cultivate the norm?
   iii. Second-order normative effects: countermeasures which may also (unintentionally) establish norms that have second-order normative effects that may clash with the long-term interests of the entrepreneur.
d) **Key Take-away:** a summary of the main findings concerning the norm development through countermeasures. This includes an assessment of the norm's position in the lifecycle, the tools of influence used to advance the norm, and the risks associated with second-order normative effects stemming from countermeasures.

3.1 Incident

Whereas the previous case study focused on Russia's hacking, this case study takes a closer look at Russian disinformation campaigns, such as those executed by state-sanctioned 'troll factories', the principal example of which is the Internet Research Agency (IRA). The U.S. was targeted by Russian campaigns both in its 2016 Presidential elections and subsequent 2018 midterm elections, constituting a serious challenge to the democratic integrity and processes of many Western countries. The most documented campaign is referred to as 'Project Lakhta' – a Russian state-sanctioned umbrella effort that used disinformation to target domestic audiences within Russia, the U.S., EU member states and Ukraine.[12] According to the U.S. Department of Justice, it operated a $35 million budget between January 2016 and June 2018, of which the last half-year constituted $10 million.[13] The Russian operatives went to extraordinary lengths to mask their location and appear as American political activists

11 Jong, de Sijbren; Sweijs, Tim; Kertysova, Katarina; Bos, Roel, "Inside the Kremlin House of Mirrors", The Hague Centre for Strategic Studies, (17 December, 2017), p. 9: https://hcss.nl/sites/default/files/files/reports/Inside%20the%20Kremlin%20House%20of%20Mirrors.pdf.
12 US Department of Justice, "Russian National Charged With Interfering in U.S. Political System", Press Release (19, October, 2018): https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system.
13 *Ibid*.

on social media platforms to create and amplify divisive social and political content and to advocate for the election or electoral defeat of particular candidates in the U.S. and European elections. Some social media accounts posted tens of thousands of messages and had tens of thousands of followers.[14] These efforts which co-opted or manufactured echo-chambers through such platforms as Russia Today (RT), Sputnik, and alt-right platforms, aimed to utilize disinformation to exacerbate existing political polarization and consequently influence the U.S. 2016 Presidential and 2018 midterm elections, as well as those of European states, such as the United Kingdom, Germany, and France.[15] Within the European context, this case will focus on the 2017 French presidential election, in which Emmanuel Macron's campaign suffered a similar Russian-orchestrated disinformation campaign – albeit with a much lower degree of success than in the United States.

3.2 Countermeasures

In responding to similar threats of Russian electoral interference, the United States and France deployed markedly different countermeasures. France largely relied on tested information security practices to slow down the attacker and engaged in a proactive debunking of disinformation, reserving its countermeasures to diplomatic statements and name-and-shaming of Russia's malign behavior. By contrast, the U.S. embarked on an aggressively offensive strategic posture, combining sanctions and indictments with the shutting down of one of Russia's primary "troll factories" for a number of days during the U.S. midterm elections in 2018, and publicly revealing a pre-deployment of cyber weapons within Russia's critical infrastructure as means to convey deterrence by punishment via coercive signaling. The U.S. countermeasures to Russian disinformation relied on several actions, including public attribution, indictments and sanctions, similar to those described in the previous case, that were issued against the IRA and other involved Russian companies such as Concord, as featured in the Mueller Report in 2018.[16] Since these measures and their underlying mandate were already described in the previous case, this case will focus more on the coercive proactive countermeasures employed by the U.S. against Russia: the shutdown of the IRA.

14 Nahzi, Fron, "The West Cannot Sit by While Russia Exploits Social Media with Disinformation", The Hill (26, December, 2019): https://thehill.com/opinion/international/475797-the-west-cannot-sit-by-while-russia-exploits-social-media-with.

15 Intelligence and Security Committee of Parliament, "Russia", Government of the United Kingdom (21 July 2020): https://int.nyt.com/data/documenttools/intelligence-and-security-committee-s-russia-report/9c665c08033cab70/full.pdf.

16 United States Department of Justice, "Russian National Charged With Interfering in U.S. Political System", Press Release (19, October, 2018): https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system.

U.S. Cyber operation against the Internet Research Agency: In February 2019, it was reported that U.S. CYBERCOM had hacked and shutdown the Russian IRA in November 2018 'for a number of days' as part of *Operation Synthetic Theology* in order to safeguard the U.S. midterm elections.[17]

U.S. Pre-deployment within Russian critical infrastructure: The United States response supplemented its initial cyber sabotage of the troll factory with a leaked report on its "pre-deployment" of cyberweapons in the Russian power grids, likely similar in scope to the reported Russian 'DarkEnergy' cyberweapon deployment in the U.S. and elsewhere.[18] Rather than 'allowing' their own pre-deployment operation to be discovered and reported by Russian actors, the U.S. self-disclosed that since 2018 they had implanted malware within Russian critical infrastructure in order to affect a kinetic-equivalent strike, if necessary.[19] The intent of this disclosure amounted to a display of coercive signaling to the Russians that the U.S. was ready to accept a level of 'mutually assured disruption'.[20]

Mandate Offensive Cyber Operations: The domestic legal basis for U.S. cyber operations is under the National Defense Authorization Act and revised 10 U.S.C. § 394, which expanded the authority of the Defense Department to operate in the cyber domain including operations "short of hostilities" and those "in areas in which hostilities are not occurring".[21] It emphasizes cyber operations as being a component of traditional military activity, for the purposes of attaining legal status as covert action – a traditionally vague area of international law may or may not consider such activities as falling under "countermeasures".[22]

Mandate U.S. Pre-deployment: The doctrinal mandate for the U.S. countermeasures derives from its doctrine of 'defend forward' and 'persistent engagement'.[23] Enshrined under the 2019 National Defense Authorization Act, this mandate approves the routine conduct of "clandestine military activity" in cyberspace, to "deter, safeguard or defend against attacks or malicious cyberactivities against the Unites States [...] before they reach their target", through continuous engagement, contestation and confrontation of adversaries throughout cyberspace that causes uncertainty wherever their adversary maneuvers.[24] Ultimately, this would allow the U.S. to gain operational advantages whilst denying them to adversaries.

French diplomatic signaling: The French response to a similar Russian disinformation campaign launched during its 2017 presidential election kicked-off with a clear signal from the French government – both publicly and through confidential channels – that it was determined to prevent, detect, and if necessary, respond to foreign

17 Nakashima, Ellen, "At Nations' Request, U.S. Cyber Command Probes Foreign Networks to Hunt Election Security Threats", Washington Post: https://www.washingtonpost.com/world/national-security/at-nations-request-us-cyber-command-probes-foreign-networks-to-hunt-election-security-threats/2019/05/07/376a16c8-70f6-11e9-8be0-ca575670e91c_story.html; Nahzi, Fron: "The West Cannot Sit by While Russia Exploits Social Media with Disinformation", The Hill (26, December, 2019): https://thehill.com/opinion/international/475797-the-west-cannot-sit-by-while-russia-exploits-social-media-with.

18 Sanger, David & Perlroth, Nicole, "U.S. Escalates Online Attacks on Russia's Power Grid," The New York Times, (15 June, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?login=email&auth=login-email.

19 Klimburg, Alexander, "Mixed Signals: A Flawed Approach to Cyber Deterrence Survival 62, no.1, (2020): https://www.tandfonline.com/doi/abs/10.1080/00396338.2020.1715071?journalCode=tsur20.

20 Maker, Simran, "Mutually Assured Disruption – Report", (12 January, 2018): https://www.ncafp.org/12606-2/.

21 United States Code, "10 U.S.C. § 394", Statues, Codes, and Regulations – United States Code: https://casetext.com/statute/united-states-code/title-10-armed-forces/subtitle-a-general-military-law/part-i-organization-and-general-military-powers/chapter-19-cyber-matters/section-394-authorities-concerning-military-cyber-operations.

22 United States House – Armed Services, "H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019", Congress.Gov: https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

23 United States Department of Defense: "Cyber Strategy 2018", (2018): https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.

24 Thornberry, Mac. "Text - H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019." (August 13, 2018): https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

Mandate Offensive Cyber Operations: In the context of international law, the 2019 Ministry of Defense "International Law Applicable to Operations in Cyberspace" formulates that France may respond diplomatically, by way of countermeasures, or employ its armed forces to repel an armed attack.[27] This constitutes the legal basis for France's adoption of "active defense"[28], which is in line with its White Papers[29] (the 2017 "International Cyber Strategy"[30], 2018 Strategic Review of Cyberdefense"[31]) and their statements within the United Nations. The term "active defense" is encompassed in the *National Defense White Paper of* 2008; it denotes a "transition from a passive defense strategy to an active defense strategy in depth, combining intrinsic protection of systems, permanent surveillance, rapid reaction and offensive action."[32]

interference. In a speech in December 2016, Minister of Defense Jean-Yves Le Drian announced the creation of a cyber command composed of 2,600 "cyber fighters".[25] A few weeks later, the minister publicly remarked that "by targeting the electoral process of a country, one undermines its democratic foundations, its sovereignty" and that "France reserves the right to retaliate by any means it deems appropriate through our cyber arsenal but also by conventional armed means."[26] Although the promise of a "retaliation by any means" never materialized – at least not in an explicitly escalatory manner – the French managed to respond effectively to the Russian disinformation threat through their preparedness and ability to a whole-of-society response that included timely and coordinated joint efforts from government and media institutions.

French information security and debunking: The Macron campaign enacted tested information security practices, including the placing of honeypots, false flags and forged documents under the pretense that they would be hacked, thereby inundating, confusing and slowing the attackers.[33] Given the tight timeframe of the elections, these measures were especially effective. The Marcon team communicated openly and extensively about the hacking and disinformation operations, gained control over the leaked information through the forged emails that they placed in honeypots, and actively debunked disinformation on social media to control the narrative. These

25 Delerue, François; Géry, Aude, "The French Strategic Review of Cyber Defense", ISPI (2 May, 2018): https://www.ispionline.it/it/pubblicazione/french-strategic-review-cyber-defense-20376.

26 Conley, Heather, "Electoral Interference", CSIS Briefs (21, June, 2018):: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

27 Roguski, Przemyslaw, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I", OpinioJuris (24, September, 2019): http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.

28 Roguski, Przemyslaw, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, PartII", OpinioJuris (24 Septmber, 2019): https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-ii/.

29 Ministry of Defence France, "Defense and National Security White Paper", (29 April, 2013): http://www.livreblancdefenseetsecurite.gouv.fr/.

30 Ministry for Europe and Foreign Affairs of France: "Stratégie Internationale de la France pour le Numérique", Diplomatie: https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

31 Secretariat-General for National Defence and Security of France, "Revue Stratégique de Cyberdéfense", Government of France (2018): http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

32 Baumard, Philippe, "Cybersecurity in France", Springer Briefs in Cybersecurity, (2017): http://www.idemployee.id.tue.nl/g.w.m.rauterberg/amme/Baumard-2017.pdf.

33 This counter-retaliation for phishing attempts is known as cyber or digital blurring and turned the burden-of-proof upon the hackers. Vilmer, Jean-Baptiste, "The "Macron Leaks" Operation: A Post-Mortem", Atlantic Council (2019): https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf; Conley, Heather A., "Successfully Countering Russian Electoral Interference", CSIS (21 June, 2018): https://www.csis.org/analysis/successfully-countering-russian-electoral-interference; Gallagher, Sean. "Macron Campaign Team Used Honeypot Accounts to Fake out Fancy Bear." Ars Technica, (5 October, 2017). https://arstechnica.com/information-technology/2017/05/macron-campaign-team-used-honeypot-accounts-to-fake-out-fancy-bear/.

debunking initiatives were not isolated to the Macron campaign team but collated around several independent researches and reliable media sources who conducted fact-checking of rumors leveled at Macron, largely from his opponent Marine Le Pen.[34] Some fake emails were so obvious that they actually helped the Macron team debunk the leaks as disinformation.[35] Furthermore, on the night of the disinformation dump, the Macron team informed the CSA, the French regulatory media authority, who asked all major news outlets to abstain from disseminating the false news. The team also informed the CNCCEP, the French electoral authorities, which issued a press release the following day asking "the media not to report on the content of this data, especially on their websites, reminding the media that the dissemination of false information is a breach of the law, above all criminal law."[36] The majority of traditional media abstained from publishing about the leaked documents or urged their readers to be cautious about the leaked documents. As a result, there was no information laundering, nor whitewashing or mainstreaming of the disinformation. Instead, the French population doubted the authenticity of the leaked documents and they generated relatively little traction compared to the United States.

Mandate Anti-disinformation: The French disinformation law, which aims to better protect democracy against the different ways in which fake news is deliberately spread, was approved in its second reading at the National Assembly on 20 November 2018. The law places special attention on the spread of disinformation during elections based on the legal definition of *fake news*, as defined in the 1881 law on the freedom of the press, in accordance with three criteria: "(i) the fake news must be manifest, (ii) be disseminated deliberately on a massive scale, (iii) and lead to a disturbance of the peace or compromise the outcome of an election". Compliance to the law will be enforced by the French Broadcasting Authority, the CSA, which is able to "prevent, suspend and stop the broadcasts of television services that are controlled by foreign states or are influenced by these states, and which are detrimental to the country's fundamental interests."[37]

Focused more on the combination of preventive cyber resilience and active debunking of disinformation than offensive engagement, the co-opting of the mainstream media by the Macron campaign and French institutions stigmatized Russia's actions and those of their collaborators, going as far as to threaten legal repercussions to outlets

34 France 24 Observers, "How We Debunked Rumours That Macron Has an Offshore Account.", (05 May, 2017). https://observers.france24.com/en/20170505-france-elections-macron-lepen-offshore-bahamas-debunked; Vilmer, Jean-Baptiste Jeangène. "The 'Macron Leaks' Operation: A Post-Mortem," Atlantic Council p. 10. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

35 Jean-Baptiste Vilmer describes the Macron team's digital blurring tactics in great detail: "One obvious example was an email supposedly originating from Macron's director of general affairs to a "David Teubey" and a "Greg Latache," both with en-marche.fr email addresses, with "bill.trumendous@cia.gov" in cc, about a plan to scrap Airbus A400M military aircraft after the election to replace them with Boeing models. That was a honey-pot story for conspiracy theorists, who see the CIA everywhere and spread claims that Macron is an American puppet. However, "David Teubey" (last name is "stupid" in verlan, an argot inverting syllables) and "Greg Latache" (last name means "the stain," a colloquial term for someone who is incompetent and useless) are characters invented by two French humorists more than a decade ago, and Bill Trumendous (Tremendous) is the CIA agent in the French spy comedy movie OSS 117: Lost in Rio. Therefore, this fake email appears to be the Macron team's attempt to humorously trap the attackers, discrediting both them and the entire leak, and have fun in the process." Vilmer, Jean-Baptiste, "The "Macron Leaks" Operation: A Post-Mortem", Atlantic Council (2019): https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.

36 Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle, "Recommandation aux médias suite à l'attaque informatique dont a été victime l'équipe de campagne de M. Macron", (May 6, 2017): http://www.cnccep.fr/communiques/cp14.html.

37 Assemblée Nationale France, "Lutte Contre La Manipulation de l'information." Assemblée nationale, (2017). http://www.assemblee-nationale.fr/dyn/15/dossiers/fausses_informations_lutte.

***Mandate Active Defense*:** The doctrinal underpinnings of France's strategic mandate are difficult to ascertain as they largely defaulted to ad hoc adaptations to the evolving scope of Russian activities. The policy of "active defense" has subsequently framed the formulation of French doctrine, in tandem with its continued policies of stigmatization and bilateral diplomatic engagement with malign state-sponsored hybrid actors. France draws a clear separation between offensive and defensive cyber operations and isolates its cyber defense agency from its wider intelligence apparatus.[44]

considering publishing the leaks.[38] The campaign decided to deny Russia Today accreditation to cover the remainder of its campaign.[39] The reason cited was their "systematic desire to issue fake news and false information" as well as their "spreading of lies methodically and systematically."[40] This is also the position the European Parliament adopted as early as November 2016.[41] Even after the election, Russian outlets have been occasionally banned from presidential and Foreign Ministry press conferences justified on the basis that these are propaganda entities and not media outlets as President Macron publicly stated following his meeting with Putin at Versailles only weeks after his election.[42] In July, 2020 Latvia's national media watchdog, the Electronic Mass Media Council (NEPLP), banned Russia Today, citing it as a propaganda outlet.[43]

Taken together, the French response successfully mitigated Russian strategic aims despite the widespread incitement of a disinformation campaign, data hacking, and large-scale leaking; there was no whitewashing or mainstreaming of the leaked data by the professional media. In contrast to the hands-off posture of the U.S. government in the 2016 Russian electoral interference, three French administrative bodies took the lead in bolstering the Macon campaign's response by offering politically neutral expertise on dispelling Russian disinformation. These were the Constitutional Council, which represents the electoral judge and body in charge of electoral integrity; the National Commission for the Control of the Electoral Campaign for the Presidential election, a campaign watchdog; and, the National Cybersecurity Agency, which operates under the Prime Minister.[45] Through these efforts, the French government successfully prevented the final stages of election meddling: there was no 'information

38 Dearden, Lizzie, "Emmanuel Macron Hacked Emails: French Media Ordered by Electoral Commission Not to Publish Content of Messages", Independent (6 May, 2017): https://www.independent.co.uk/news/world/europe/emmanuel-macron-email-hack-leaks-election-marine-le-pen-russia-media-ordered-not-publish-commission-a7721111.html.

39 Reuters, "Emmanuel Macron's Campaign Team Bans Russian News Outlets From Events", Guardian (27, April, 2017): https://www.theguardian.com/world/2017/apr/27/russia-emmanuel-macron-banned-news-outlets-discrimination.

40 Smith, Rachel Craufurd, "Fake News, French Law and Democratic Legitimacy: Lessons for the United Kingdom", Journal of Media Law, (11)1, (2019): https://www.tandfonline.com/doi/abs/10.1080/17577632.2019.1679424?af=R&journalCode=rjml20

41 European Parliament, "European Parliament resolution of November 23, 2016, on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI))", EUR-LEX (23 November, 2016): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016IP0441.

42 France24, "Video: Macron Slams RT, Sputnik News as 'Lying Propaganda' at Putin Press Conference", (30 May 2017): https://www.france24.com/en/20170530-macron-rt-sputnik-lying-propaganda-putin-versailles-russia-france-election

43 Gehrke, Laurenz, 'Latvia Bans Russian Television Channel RT', Politico (1 August, 2020): https://www.politico.eu/article/latvia-bans-rt-russian-television-channel/.

44 Guiton, Amaelle, "Cyberattacks: Paris and Moscow Face to Face", Libération (11 November 2018): https://www.liberation.fr/planete/2018/11/11/cyberattaques-paris-et-moscou-en-tete-a-tete_1691473.

45 Vilmer, Jean-Baptiste, "The "Macron Leaks" Operation: A Post-Mortem", Atlantic Council (2019), p. 39: https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.

laundering', nor mainstreaming or whitewashing of the disinformation, the process by which traces of foreign interference are removed from the information narrative. As respective approaches to a mutual problem, the U.S. and French represent archetypes of alternative doctrines, specifically in their divergence along lines of "persistent engagement" versus "active defense".

In summary, both U.S. and French countermeasures share tactics of stigmatization, denial and, in the case of the U.S., reciprocal punishment. The U.S. had previously shown to be largely unprepared for the efficacy and scope of Russian disinformation in its 2016 presidential election. The subsequent coercive actions of U.S. CYBERCOM directed at the Internet Research Agency reinforce a more assertive posture enshrined in their 'defend forward' and 'persistent engagement' doctrine. The additional step by the U.S. to disclose its penetration into Russian critical infrastructure (rather than being caught in the act), with the implication that it had established a form of deterrence through imposed reciprocal cost to Russia, is a distinct form of coercive signaling. France made effective use of digital blurring to mitigate the utility of stolen data; this preventive resilience contrasts with the more aggressive U.S. posture. Where the U.S. adopted a militarily conceived direction of denial-through-engagement and enacting deterrence through the threat of 'mutually assured disruption', the French strategic posture effectively turned Russian strategy against itself, removing the political utility of its information warfare. The following section evaluates these differences through the lens of their respective normative implications, and the role of actors as emergent norm entrepreneurs.

3.3 The Normative Dimension: What Norms are Promoted?

The U.S. and French actions were aimed at derailing or delegitimizing Russian disinformation by denouncing and breaking a pattern of behavior that could otherwise establish a norm. As of now, disinformation is not explicitly illegal according to international law, nor is there a norm that emerged specifically dedicated to the tackling of disinformation. In lieu of an explicit norm, the norm lifecycle cannot be applied. Instead, this section will predominantly focus on the application of existing international norms and legal principles that can be used as *linking* or *framing* tools to explore the viability of a norm against disinformation. To this end, the fundamental principle of state sovereignty is the starting point. Finally, the second-order normative effects of the French and U.S. countermeasures will be evaluated to see if they conflict with their long-term interests.

3.3.1 Affirmation of Existing Norms?

Sovereignty. Some may believe that the principle of sovereignty already erects a normative barrier to Russia's disinformation efforts. In its response, France linked the disinformation campaign to the norm of sovereignty, stating that "by targeting the electoral process of a country, one undermines its democratic foundations, its sovereignty".[46] In addition, the specific ruling that "the principle of sovereignty applies to cyberspace" equates sovereignty in cyberspace with traditional notions of territorial sovereignty, the use of force, and non-intervention by one state into the territory of another.[47] Within the cyber discourse, there remains an ongoing debate as to whether sovereignty itself is an enforceable rule of international law or merely a principle of international law.[48] France is among the former group and holds that "any unauthorized penetration by a state into French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty".[49] Austria, Germany, the Netherlands and the Czech Republic also agree with the sovereignty-as-a-rule interpretation, albeit with varying degrees as to what kind of activity would automatically constitute a violation of sovereignty. By contrast, the U.S., like the U.K., holds the view that sovereignty is merely a principle of international law and does not create autonomous and separate legal obligations, but is protected by other established rules of international law, such as the prohibition of the use of force or the principle of non-intervention.[50] Without going into the legal details of this debate, it is clear that the principle of sovereignty would offer little relief by itself — the purported rule suffers from much ambiguity with respect to state cyber and information operations.[51]

Nonintervention. Article 2(4) of the United Nations Charter articulates the nonintervention rule and elevates it as a principle of legal, and thus, binding character.[52] Whereas the norm proposed in the previous case study was linked to article 2(4) through the prism of cyberspace, this case study analyzes it through the prism of

46 Jean-Yves Le Drian (minister of defense), interviewed in Le Journal du Dimanche, "France Thwarts 24,000 Cyber-Attacks Against Defence Targets", BBC, (8 January, 2017): https://www.bbc.com/news/world-europe-38546415.

47 Ministére des Armées, "International Law Applied to Operations in Cyberspace": https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf#page=6.

48 Roguski, Przemyslaw, "The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States", Just Security (11 May 2020): https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

49 Ministry of Defense France, "International Law Applied to Operations in Cyberspace": https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf#page=6.

50 Roguski, Przemyslaw, "The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States", Just Security (11 May 2020): https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

51 Corn, Gary: "Coronavirus Disinformation and the Need for States to Shore Up International Law", Lawfare (2 April 2020): https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law.

52 United Nations, "Charter of the United Nations," (10 August 10, 2015). https://www.un.org/en/charter-united-nations/.

the information environment.[53] Article 2(4) of the UN Charter states that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[54] Traditional understandings link the prohibition on the use of force to an element of armed force involved, or at least actions resulting in physical injury or damage. Russian hybrid operations exploiting the gray zone have generally sought to test the response thresholds of their opponents and steer clear of causing physical harm, at least in the cyber and information environment, and thereby from tripping over the use-of-force threshold.

Cyber operations can reach the threshold at a loss of life and significant economic harm, which has been reaffirmed by a growing number of states, including the Netherlands and France.[55] States, however, have been less open about the application of this threshold to disinformation – a form of statecraft not prohibited under international law. They have not and are unlikely to deem Russia's spread of disinformation as a use of force. Doing so would mean that they agree with the Russian and Chinese interpretations of use of force that includes psychological and media warfare.[56] Russia's and China's perceptions of information as a weapon consider bad *content* as critical or dissenting of the regime and thereby as an attack against the state.

The principle for nonintervention in the internal affairs of other states is, however, well-established within customary international law. It allows states to safeguard their sovereignty and independence, and its application to cyberspace has been established and reinforced by many states.[57] Like the use-of-force prohibition, the nonintervention

---

53 For a definition of the information environment, see US JP-3-12 Cyberspace Operations: "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.", Joint Staff. "Joint Publication 3-12: Cyberspace Operations." JCS.mil, (8 June, 2018): https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.; Cyberspace is considered to be part of the information environment, and is defined by the Netherlands Military Cyberspace Doctrine in the same way as the NATO AJP 3.20 allied Joint Doctrine for Cyberspace Operations: "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data." Ministry of Defense of the Netherlands, "The Netherlands Armed Forces Doctrine for Military Cyberspace Operations". Dutch Defense Cyber Command, (June 2019).

54 *Ibid.*

55 Government of The Netherlands, "Appendix: International Law in Cyberspace", (26 September, 2019): https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf ; Ministére des Armées, "International Law Applies to Operations in Cyberspace", (24 September, 2019): http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/#:~:text=As%20a%20permanent%20member%20of,international%20law%20applies%20to%20State.

56 Cruz, Taylor; Simoes, Paulo, "EECWS 2019 18th European Conference on Cyber Warfare and Security", Academic Conderences and Publishing Limited, (4 July, 2019): https://books.google.nl/books?id=b8-hDwAAQBAJ&pg=PA690&lpg=PA690&dq=RU+ISD+2000&source=bl&ots=KOV-FEKixs&sig=ACfU3U3t7xJ9jzukeCskclpbZqc-H81P_Q&hl=en&sa=X&ved=2ahUKEwjy5-6rglLHqAhVNy6QKHfyiA00Q6AEwAHoECAgQAQ#v=onepage&q=RU%20ISD%202000&f=false.

57 The International Court of Justice (ICJ) has described the principle of non-intervention as "a corollary of every state's right to sovereignty, territorial integrity and political independence," and of the right, as a matter of sovereign equality, of every state to conduct its affairs without outside interference. International Court of Justice, "Case Concerning Military and Paramilitary Activities in and Against Nicaragua", (1986): https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

rule is considered to be of limited scope. Fundamentally, it prohibits the use of *coercive* measures to overcome the free will of a targeted state with respect to matters that fall within that state's core, independent sovereign prerogatives.[58] "Unfortunately, the concepts of coercion and "domaine réservé"—the bundle of sovereign rights protected by the rule—are ill defined".[59] Such ambiguities can be cleared up by states disclosing their official views and interpretations. Thus far, only a handful of states have done so on the application of the nonintervention rule in cyberspace and even less for the information environment. The most concrete statements that go beyond a general acknowledgment that the parameters of the rule 'have not yet fully crystallized in international law' is the manipulation of electoral processes and the COVID-19 *infodemic*.[60] The United Kingdom goes further in its statement that an intervention in the fundamental operation of Parliament or in the stability of the financial system would "surely be a breach of the prohibition on intervention."[61]

Arguably, disinformation campaigns that aim to sow discord, distrust, and societal division do not instantly lead to a conclusion of *coercion* as individuals are free to accept and reject information they come across. Nonetheless, the national mandate for the countermeasures described earlier can provide guidance to the clarification of the coercion element. By linking Russian disinformation in 2016 to fraud and deceit, Special Counsel Robert Mueller's indictment demonstrates that covert deception and disinformation can be just as harmful to sovereign prerogative as more overt coercive measures, if not more so.[62] It also reinforces that election processes are a paradigmatic example of the type of sovereign prerogatives protected by the nonintervention rule, leading some legal experts to assert that Russia's election interference crossed a red line.

---

58 Interventions against the sovereignty and the principle of non-intervention require an element of coercion. This concept can be defined broadly or narrowly, with great consequences for the analysis of the case. Unfortunately, international law says very little about the theory of coercion. A complete analysis of what constitutes coercion within this context of international law is too expansive for this study. For more information about this, see Ohlin, Jens David, "Did Russian Cyber Interference in the 2016 Election Violate International Law?," 95 Texas Law Review 1579 (2017): https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2632&context=facpub; Hollis, Duncan B, "The Influence of War; The War for Influence." SSRN Scholarly Paper, Social Science Research Network, (3 April, 2018): https://papers.ssrn.com/abstract=3155273.

59 Corn, Gary, "Coronavirus Disinformation and the Need for States to Shore Up International Law", Lawfare (2 April 2020): https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law.

60 The Netherlands referenced to the principle of non-intervention when it called out Russian disinformation campaigns during the COVID-19 pandemic. UNODA. "The Kingdom of the Netherlands' response to the pre-draft report of the OEWG" (April 2020). https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf; Corn, Gary: "Coronavirus Disinformation and the Need for States to Shore Up International Law", Lawfare (2 April 2020): https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law.

61 Attorney General's Office; Wright, Jeremy: "Cyber and International Law in the 21st Century", Government of the United Kingdom (23 May 2018): https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

62 Corn, Gary; Jensen, Eric: "The Technicolor Zone of Cyberspace – Part I", Just Security (30 May 2018): https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part/.

3.3.2 A New Norm Emerges?

In lieu of an explicit norm, this section offers suggestions for *framing* and *linking* a potential disinformation norm for entrepreneurs, as well as the first steps to assist in socialization. This is obviously just one approach that need not frame a 'final norm' to the overarching problem of disinformation. But it may form a beginning.

Linking disinformation to the nonintervention principle. The principle of sovereignty offers a good starting point but little relief by itself given the ongoing debate as to whether sovereignty itself is an enforceable rule or merely a principle of international law. Instead, election meddling is one of the few forms of disinformation that appears to reach the *coercion* threshold of the nonintervention principle on the basis of official statements or responses from Western like-minded countries.[63]

Framing disinformation as covert election interference. The norm should be framed in such a way that it prohibits concerted Russian *covert* disinformation and influence campaigns aimed at undermining democratic processes while allowing the U.S. and its partners to both allow and sanction *overt* tools to influence elections, for instance by supporting the civil society in the targeted country through formal means, or the informal support of one's own civil society. To this could be added other positive inducements such as trade policy and foreign aid to maintain government and foreign support. Research shows that in contrast to the covert Russian threat described in this case study, most post-Cold War election interference by the United States has been overt, including open support to civil society and democratic processes and aiding governments in the hopes of supporting their reelection.[64] Authoritarian regimes, such as Russia, would favor a policy of *total* nonintervention and noninterference in the international affairs of other countries. It would keep Western democracy promotion, support to civil society, aid to opposition parties, public criticism of the Russian regime at bay and offer the Kremlin nearly unopposed internal control.[65] The suggestion above would form a compromise of sorts: overt means of any sort, including 'propaganda' by

63 Morris, Lyle J., Michael J; Mazarr, Jeffrey W; Hornung, Stephanie Pezard; Anika Binnendijk, and Marta Kepe. "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War." RAND, (2019) https://www.rand.org/pubs/research_reports/RR2942.html.

64 Shimer, David, "Rigged: America, Russia and 100 Years of Covert Electoral Interference", Harper Collins U.K., (2020): https://books.google.nl/books/about/Rigged_America_Russia_and_100_Years_of_C.html?id=xjDZDwAAQBAJ&redir_esc=y; Beinart, Peter: "The U.S. Needs to Face Up to Its long History of Election Meddling", The Atlantic (22 July 2018): https://www.theatlantic.com/ideas/archive/2018/07/the-us-has-a-long-history-of-election-meddling/565538/; Shane, Scott: "Russia Isn't the Only One Meddling in Elections. We Do It Too", New York Times (2018): https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html.

65 In 2018, Russia proposed a resolution at the United Nations General Assembly, which some argue legitimizes state surveillance and censorship through its emphasis on sovereignty and non-interference in the internal affairs of countries—terms which have been used by governments to cover up measures that infringe on human rights online. Council on Foreign Relations, "The Sinicization of Russia's Cyber Sovereignty Model", (1 April, 2020): https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/#footnote_5_3341; Council on Foreign Relations, "The Sinicization of Russia's Cyber Sovereignty Model", (1 April, 2020): https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model.

state media actors such as RT (or from a Russian point of view BBC or CNN), would be considered acceptable, as would however publicly declared funding of civil society organizations (including, for instance, the U.S. National Endowment of Democracy or the Russian Russkiy Mir Foundation) but would disclaim hidden subterfuge including clandestine 'civil society' funding, hacking, or non-transparent strategic communication.

Start with a unilateral ban. Robert Knake suggests that the U.S. government takes unilateral action in order to shape global norms in a similar way as the norm against commercial IP theft or political assassinations.[66] He believes U.S. Executive Order 12333 on "United States Intelligence Activities" that bans assassinations would be an expeditious way to internalize and socialize the norm within the U.S. intelligence community and keep the intelligence community from participating in covert election interference. It would not only allow a first-mover advantage in framing the issue but would also combat the perception that liberal democracies such as the U.S. conduct covert influencing activity. The national intelligence community can be persuaded by linking the value of such a norm to the national security interests: "In an era in which election interference tools are not held in a Cold War duopoly but are globally available, creating a strong norm against clandestine interference in democratic processes is in the national security interest of the United States."[67]

Acquire broad support. The entrepreneur should use a coalition or alliance as an organizational platform to socialize the norm with partners and lay the groundwork for opening discussions with Russia on their elections interference and to sanction countries that continue to covertly interfere in elections. "As with the agreement with China on economic espionage, the United States and allies would need to agree to abstain from covert election interference even if they are already not doing so in order to allow the Russian government sufficient cover to present any agreement to its citizens as a triumph for Russia."[68] With a broadly supported norm, the United States will be better positioned to create a coalition to punish Russia and other nondemocratic states when their disinformation campaigns covertly interfere in democratic processes.

3.3.3 Second-Order Normative Effects of the Countermeasures

States may underestimate or even be unaware that countermeasures may establish new norms that conflict with their own long-term interests. As these norms are in their early emergence, they, and the countermeasures which initially formed them, may produce unanticipated long-term consequences. We will take a closer look at how these effects impact the long-term interests of the states that undertook the

66 Knake, Robert, "Banning Covert Foreign Election Interference", Council on Foreign Relations (2020): https://www.cfr.org/report/banning-covert-foreign-election-interference?utm_medium=social_share&utm_source=tw.
67 *Ibid*.
68 *Ibid*.

countermeasures and the normative initiatives of their opponent. In this case study, we identify three negative externalities associated with the respective countermeasures that run contrary to the interests of the entrepreneur. These are mainly concerned with the second-order effects of overt pre-deployment in adversary systems on introducing a norm of mutual-hostage taking, of overt offensive cyberspace operations in response to disinformation and their effects on the weaponization of information, and finally the labeling of media outlets as propaganda.

Pre-deployment in Russian critical infrastructure establishes a norm of 'mutually assured debilitation'. The unilateral action of the U.S. in pre-deploying within Russia's electrical grids did not occur in a normative vacuum. Clearly, it violated Russia's sovereignty for doing something that is not strictly illegal according to international law. It reaffirms that the U.S. considers sovereignty in cyberspace as more a baseline principle to inform modes of responsible behavior, rather than a set rule. At the same time, it is unlikely that American prepositioning within the Russian power grid constitutes an official renunciation of the agreed UN norm prohibiting cyber operations that damage critical infrastructure.[69] While it may have intruded into the system, U.S. CYBERCOM did not carry out an attack that damaged the critical infrastructure but implicitly threatened such action in order to impose costs sufficient to alter Russian behavior.[70] Even if it does not constitute a direct renunciation of existing norms, it conveys a lack of sincere commitment or double standard that critical infrastructure *may* be included as part of cost imposition against adversaries.

The American public declaration of its willingness to significantly violate the sovereignty of an adversary in peacetime seems to present a novel situation for international law. In an analysis of the U.S. persistent engagement doctrine, Alexander Klimburg describes this second-order effect as follows: "By effectively declaring that the United States considered the pre-deployment of cyber weapons within an adversary's critical infrastructure as permissible (rather than simply being 'caught in the act', as the Russians were), CYBERCOM deviated from the established international legal order that the United States has helped to create." He goes on to say that "It also implicitly accepted a norm of mutual hostage-taking or 'mutually assured debilitation', a huge strategic concession that implies US' acceptance of a level of parity with adversaries

69 The UN General Assembly endorsed a set of norms established in 2015 by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), which includes a norm prohibiting cyber operations that would damage critical infrastructure: "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (22 July, 2015): https://undocs.org/A/70/174.

70 Schmitt, Michael, "U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?" Just Security, (June, 18, 2019), https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/.

where previously it could insist on hegemony."[71] Furthermore, these actions imply that CYBERCOM, and possibly the entire U.S. government, has accepted that 'peacetime' and 'wartime' are artificial distinctions, particularly in the context of the strategic asymmetric domain of cyberspace, reinforcing the Russian and Chinese strategic narratives.

By responding to disinformation with kinetic cyber effects, the U.S. perceives and weaponizes information in the same way as Russia. Klimburg also describes the effects of CYBERCOM's response to the weaponization of information.[72] Although they may have fallen below the threshold of the 'use of force' or 'armed attack' – a distinction not usually made in the United States – they conveyed a public message implying that it is now acceptable to hack what you consider 'fake news' and the weaponization of information. If Russian disinformation is not linked to violations of international law, the U.S. may, through its own countermeasure, undermine existing international law in favor of Russian and Chinese interpretations that argue in favor of negotiating 'good' and 'bad' content. If targeting actors that have a disinformation function, such as the Internet Research Agency, becomes normalized, then similar attacks by Russia and China on conventional media organizations, civil society, and other NGOs may follow. Klimburg explains that Moscow may consider U.S. support for Russian civil society as 'information and psychological actions aimed at undermining the homeland'.[73] Similarly, Beijing may consider Chinese translations of U.S. newspapers provocative. The new U.S. doctrine and its countermeasures may, therefore, encourage disputes about 'bad content' and lead to the very thing it was intended to alleviate: the weaponization of information.[74]

Media outlets may be labeled as propaganda by political figures. Whilst the actions of the Macron campaign to curtail the well-documented disinformation operations by Russian outlets such as Russia Today were effective, their method of doing so harbors the second-order prospect that other states may employ similar methods against legitimate media outlets. The subsequent efforts of the EU to establish an independent body to track disinformation hints at an attempt to depoliticize the process of designating fake news. However, the normative precedent set by the Macron campaign persists – that media outlets may be labeled illegitimate by political figures or campaigns. Macron's announcements that fake news represents a threat to democracy provides credence for other countries to make the same normative claim, banning or

71 Klimburg, Alexander, "Mixed Signals: A Flawed Approach to Cyber Deterrence," Survival 62, no. 1 (2020): https://www.tandfonline.com/doi/abs/10.1080/00396338.2020.1715071?journalCode=tsur20.
72 *Ibid*.
73 Ministry of Foreign Affairs of Russia, "Doctrine of Information Security of the Russian Federation", (5 December, 2016), p. 44: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
74 Klimburg, Alexander: "Mixed Signals: A Flawed Approach to Cyber Deterrence" Survival 62, no.1 (2020): https://www.tandfonline.com/doi/abs/10.1080/00396338.2020.1715071?journalCode=tsur20.

restricting any media they deem as 'fake'. While Western media civil society and NGOs may now be labeled as Western propaganda machines in a similar way, the second-order normative effects are not as profound or further-reaching as the U.S. effects on the weaponization of information.

3.4 Key Takeaways

In lieu of explicit legal and normative guidelines prohibiting disinformation, the West should frame the respective norm around covert election interference and link it to the nonintervention principle. Doing so would first prohibit concerted Russian covert influence operations aimed at undermining democratic processes while allowing Western overt tools. It should not favor the authoritarian regimes' policy of total noninterference — no democracy promotion, no support to civil society, no public criticism. Second, it would reinforce the rules-based order, shape normative behavior, and potentially deter Russia and other states from engaging in similar behavior going forward. Second, it would bring greater clarity and weight to the nonintervention rule. Russia and other states would be put on notice that covert election interference falls within the set of sovereign prerogatives protected by the rule. It would also advance the view that covert deception campaigns aimed at overcoming sovereign free will, effectively by means of fraud, can constitute coercion even in the absence of actual force. Finally, under the law of countermeasures, it would expand the choice of permitted response measures by affected states.

In order to avoid risky second-order normative effects, countermeasures to disinformation should refrain from imposing overt kinetic effects. The U.S. doctrine of 'defend forward' and persistent engagement oriented itself around the imposition of costs, directly compromising Russian troll factories and using coercive signaling via pre-deployment in its electrical grids. It thereby conveyed a *public* message implying that it is now acceptable to hack what you consider 'fake news' thereby encouraging disputes about 'bad content'. Ultimately, this may lead to the very thing the doctrine was intended to alleviate: the weaponization of information. Furthermore, by openly communicating about their pre-deployment (rather than being caught in the act) it designated critical infrastructure as a viable vector of coercive signaling - that the range of acceptable cyber targets had expanded to include critical infrastructure, up to the point of threatening 'mutually assured disruption'. Without recognition of the second-order effects of countermeasures upon the wider cyber and information environment, unintended consequences may undermine the very goals states wish to achieve, and render the broader information security environment more uncertain, hostile and complex. As a comparative case study in countermeasures, the U.S. approach produced a variety of dangerous precedents that will likely inform future calculations of other actor's behavior in cyberspace.

4. Conclusions and Recommendations From the Paper Series

Hybrid conflict is characterized by the deployment of activities that occur across domains, overtly and covertly, including economic coercion, disinformation campaigns and cyberattacks. They are intended to circumvent detection, existing laws, and response thresholds to minimize the basis for decisive responses. Western countries that are on the receiving end of such activities are trying to counter them using a portfolio approach ranging from preventive resilience to proactive response and punishment of hybrid violations.

This report has considered the strategic utility of norms in shaping adversarial hybrid conflict behavior. Norms function via an actor's self-perception, their interests, values, and fear of stigma or material costs from other adherents in the international community if they do not conform to the norm. It is crucial to gain a better understanding of how norms develop and what states can do to support this process. To that purpose this report has used the norm lifecycle from academic literature to describe the process of norm development, starting from norm emergence towards norm cascade and internalization.

Typically, a norm emerges either out of habit or as the result of advocacy by *norm entrepreneurs* who *frame* their norm within a specific context and *link* it to other norms, laws or principles that reflect their interests. *Organizational platforms*, such as the EU, UN, or SCO, are often used to accelerate the *socialization* of a norm. At the same time, these platforms limit the scope and audience of the norm, thereby potentially barring it from broader acceptance. This report has outlined three strategies that can be used to promote norms: *socialization*, *persuasion,* and *coercion*. Socialization leverages the shared relations and identities between actors and institutions in order to push a norm towards conformity. Persuasion denotes the promotion of a norm through positive material incentives and/or immaterial incentives, such as *linking* and *framing*. Coercion encompasses the use of or threat of negative inducement toward another into accepting a norm.

The report then applied the norm lifecycle and the strategies of influence to five real-world case studies specifically looking at the promotion of norms by states in the context of countermeasures in response to hybrid threats. The premise of the report is

that countermeasures should be carried out in a responsible way, have an underlying legal or normative basis, and take into consideration the second-order normative effects which have often been underestimated or even ignored. In doing so, it analyzed a wide range of Western countermeasures in response to Russian and Chinese hybrid threats and assessed the norms that emerge from such countermeasures. The sample of cases was both too small and too diverse to draw generic conclusions about particularly effective combinations of strategies. Furthermore, because the case studies describe relatively young norms that are still under development, it is not yet possible at this stage to determine what combination of strategies may work best under what circumstances. An area of further research, therefore, includes the application of the lifecycle to a wider set of cases, including historical ones, within the context of interstate strategic bargaining that allows for the identification of best practices. At the same time, the richness of the cases certainly yielded a set of important insights concerning the role of norms in shaping hybrid threat behavior and the ways in which state entrepreneurs can build their strategies across the different phases of the norm lifecycle.

First and foremost, our analysis warrants the conclusion that norms are in fact relevant instruments to shape adversarial hybrid behavior. They by no means constitute a silver bullet and their emergence, cascade, internalization and sustenance require a concerted effort on the part of norm entrepreneurs. Norms cannot be launched and left to fend for themselves. They are not fixed products of agreements, nor are they static nodes of international relations. A norm previously taken for granted may come to be viewed as wholly objectionable given the passing of time and/or changing circumstances. Norms, therefore, need to be continually promoted by their norm entrepreneur, and that entrepreneur must continue to exercise leadership in building support and widening the like-minded coalition behind it. Historically it has been difficult to "transfer" leadership on a norm issue, even when there are other actors willing to step in.

Second, habit and repetition alone – in particular when they go unchallenged – create new norms, and similar norms reinforce each other. This not only applies to the hybrid threat actor – for example, China normalizing IP theft – but also to the victim undertaking countermeasures that denounces and breaks a pattern of behavior to keep the hybrid actor from establishing new norms. Similar norms of habit – be it towards violating sovereignty using cyber but also conventional means, for example – therefore reinforce each other. Likewise, similar norms of cooperation or prohibition – for instance towards protecting parts of civilian critical infrastructure in peacetime – tend to reinforce each other. If there are no adverse consequences for those who violate accepted norms, those norms become little more than words on paper and in time they may be challenged and changed as new habits take place.

Third, and in line with the second point, countermeasures typically have second-order normative effects which can cause problems. These effects can be more profound when states execute overt coercive countermeasures in peacetime, which can not only lead to direct tit-for-tat escalation but can also help set contrarian norms – like equating disinformation to kinetic operations. Our analysis clearly highlights the need for states to take the long-term strategic risks of second-order normative effects of countermeasures into consideration when they decide on their policy options in response to hybrid threats. It is important to view these consequences in the context of their impact upon the long-term strategic goals of the actor, particularly in how they set new precedents for escalatory responses in peacetime. We offer the observation that overt coercive countermeasures (including the leaking of covert measures) have the largest propensity for inadvertent effects, but that this risk can sometimes be mitigated by pursuing a simultaneous multi-fora diplomatic strategy.

Fourth, the promotion of norms is context-specific and its success rests not just in its content but in its process: who pushes it, what identity is associated with it, how and where is it pushed, on which basis (political, legal, ideational), and finally who accepts it and the reason why they do so. The case studies reinforce Finnemore's notion that process *is* part of the product. Our analysis has only started to unpack some of the strategic dilemmas and trade-offs that shape the process and the adoption of norms in the hybrid realm. Because the norm-setting process within this field is relatively young, it is too early to tell whether there are more general precepts that can be established down the line. Yet, policymakers should be conscious that these choices affect their desired end result.

Fifth, norms can be spread or internalized by single or multiple tools of influence simultaneously – spanning persuasion (linking, framing and (material) incentives), coercion (threats, sanctions or indictments), and socialization (mimicry, bandwagoning, stigmatization). An entrepreneur should take advantage of the wider spectrum of tools and realize where they enforce their strategy or potentially crowd out other tools. Each tool comes with its own set of costs and benefits that require the entrepreneur to continuously (re)evaluate their choices based on their interests and changing contexts.

Sixth, entrepreneurs should adopt multilevel approaches to norm promotion that synchronize measures at the political, strategic, and tactical level. When the U.S. pursued a norm against economic cyber espionage, it first aimed to pursue it diplomatically through the United Nations. When that was turned down by Beijing, the U.S. opted for more coercive measures at the tactical (indictments) and strategic level (threat of sanctions) while exerting high-level political engagement (President Obama and Xi) that led to a bilateral agreement. While it operated across different domains and at various levels, the U.S. signaled consistently and uniformly to Beijing that cyber-enabled IP theft is unacceptable, and that the U.S. was willing to escalate

the issue while at the same time offering incentives for norm confirmation. This approach not only provided multiple avenues for reinforcement, it also contained the risk of inadvertent second-order effects, even when overt moves were employed. In contrast, the later U.S. strategy of persistent engagement was highly limited in its communication and engagement, employing a volatile mix of covert military effects and the overt disclosure of them, and consequently led to mixed signaling and a broad range of unintended and undesirably second-order normative effects.

Seventh, norm processes take time, effort and resources. Entrepreneurs should therefore have a clear long-term strategy in mind that takes into consideration the costs and timeframe of their strategic dilemmas, trade-offs, and tools of influence. For example, establishing new organizational platforms or persuasion through material incentives are costly options reserved for powerful or resourceful states. These are particularly relevant when entrepreneurs face opposition or countermobilization from other actors or when they deal with actors with very different value and interest systems – which makes it is extremely difficult to persuade them unless the norm is incompletely theorized.

Eighth, in order to facilitate norm cascade and internalization, entrepreneurs should strive to create broad coalitions which go beyond classic like-minded groups of states, and which represent true communities of interest of state and non-state actors. Together, these actors are better placed to isolate and call-out hybrid threat actors, stigmatize particular forms of behavior and mobilize support to impose costs on norm transgressors. Imposing costs for norm violations should also have a strong direct link to the violation rather than a sweeping broad range campaign that may lead the target to believe they have little to gain from continuing to honor the agreement. Rather than imposing unilateral costs, a state should mobilize large-scale responses utilizing the much wider resources of private sector and civil society actors that have joined the respective communities of interest. If a state sticks to government-to-government approaches it not only significantly limits the variety of response options that can be taken against the norm-violator, but it may also unnecessarily sacrifice additional legitimacy by failing to bring in other allied voices. In consequence this can also weaken a state's position vis-à-vis other friendly states, who may then not render the political support necessary, risking the degeneration of the norm violation purely into that of a bilateral issue. Further research is required as to how states can better leverage coalitions with non-state actors from the private sector and civil society to pursue norm adoption, implementation, and enforcement, an area which clearly seems to be a force-multiplier not only in building legitimacy for a norm, but also in increasing the scope of punishment for a transgressor.

Ninth, in countering the urgent challenge of disinformation and election meddling, we suggest that analysts and policymakers apply the insights concerning norm

promotion identified in this study when developing a norm. As discussed in case study two, Western governments have highlighted the threat of disinformation within the context of undermining democratic processes, while Russian strategies, doctrines and thinking simultaneously highlight the potential threat of (Western) information and influence campaigns to the Russian regime. If it is determined that such a norm can be useful, Western analysts and policymakers should develop a norm strategy that links and frames the norm to a context that reflects its own interest and values, seek broad support for the norm from its partners, and engage diplomatically, with Track 2 diplomacy as a potential starting point, to facilitate strategic bargaining with Russia and China.

Tenth, and finally, policymakers should recognize that while we find ourselves in a hybrid conflict, it is important not to exacerbate it unnecessarily with responses that escalate the conflict beyond what is required to safeguard Western interests. Russian and Chinese hybrid operations test Western response thresholds within a gray zone that spans the border between wartime and peacetime. The Russian and Chinese *forever war* doctrine is based on the Leninist view that politics is an extension of war by other means. It implies that *all* measures are on the table at *all* times. It also reverses the Clausewitzian thinking of war as an extension of politics that implies a separation between peacetime and wartime, which lies heart of the international legal and security framework that Western liberal democracies established. Within this space, the migration of Western wartime countermeasures to the peacetime environment leads to higher second-order normative effects that undermine the West's long-term strategic interest in upholding the nature of the existing international legal order. Succumbing to the desire to respond in kind to hybrid attacks, therefore, may not only be tactically and operationally difficult, but strategically and politically unwise: it would reinforce the Leninist forever war doctrine that rejects not only international law and the rules-based order, but the very notion of a mutually beneficial win-win (rather than a zero-sum) world. In such a world, maximum escalation strategies would be a logical choice – until, of course, they go wrong.

We offer the following recommendations for democratic governments seeking to use norms as part of a wider strategy to respond to challenges in the sphere of hybrid conflict. We stand only at the beginning of the process of developing effective norms that can limit state and non-state behavior in this sphere. These recommendations are designed not to finalize that process, but to take the next positive steps forward, as part of a concerted norm campaign to shape hybrid threat behavior of adversaries:

1. **Determine shared restraints on state action to help promote norms by behavior.** As noted in this report, one way in which norms arise is through restraint in state action – sometimes explicitly developed, sometimes organically emergent – which helps, through repeated patterns of behavior, to formalize a norm. European

Union members and NATO allies in particular, in partnership with value-sharing democracies including Japan, India, South Korea, Australia and many others, should discuss specific forms of hybrid restraint they are willing to undertake – actions they agree to forgo – as part of a campaign to promote norms.

2. **Develop joint commitments that go beyond classic like-minded groups of states to punish unacceptable behavior in the hybrid competition but do so cognizant of the risks of unintended consequences.** Norms gain strength in part through active enforcement. When they are enforced by a community of interest, the state and non-state actors involved are better placed to isolate and call-out hybrid threat actors, stigmatize particular forms of behavior and mobilize support to impose costs on norm transgressors. These communities can begin to identify behaviors they will seek to punish in this domain—a trend that is already well underway in the area of Russian disinformation and to some degree with regard to Chinese coercive maritime activities. A community of interest working to promote norms could accelerate this process with more explicit commitments of punitive responses to particular forms of hybrid aggression.

3. **Sponsor Track 1.5 / Track 2 dialogues to identify specific behaviors that will be considered irresponsible in the hybrid conflict space.** A norm proposal against disinformation could be *framed* around covert election interference and *linked* to the nonintervention principle, which would prohibit concerted Russian covert influence operations aimed at undermining democratic processes, while allowing overt support for democratic processes and voices. One near-term step would be for broad-based coalitions of democracies to support non-governmental dialogues to help define the most feasible and potent set of norm proposals for further action. These dialogues should consciously address issues of unintended consequences raised in this report, including the second-order normative effects.

4. **Direct resources to groups and individuals serving as norm entrepreneurs that serve as a force-multiplier for building legitimacy for a norm, but also in increasing the scope of punishment for a transgressor.** This will enable states to better leverage coalitions with non-state actors from the private sector and civil society to pursue norm adoption, implementation, and enforcement. Democracies should increase the funding and other support for communities of interest that help drive norm emergence and cascading. These include civil society commissions that develop norm proposals, organizations devoted to fighting disinformation, groups that use open-source intelligence to name and shame hybrid threat attacks, and research organizations studying the content of helpful norms. Even before the final shape of proposed norms becomes clear, such norm entrepreneurs can help advance the general appreciation for the issue required for norms to emerge and become socialized.

The Hague Centre for Strategic Studies

info@hcss.nl

hcss.nl

Address:
Lange Voorhout 1
2514EA
The Hague
The Netherlands