The Hague Centre for Strategic Studies

HCSS PAPER SERIES – CASE STUDY 1

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 1: Protecting Electoral Infrastructure from Russian Cyberoperations

The Hague
Centre for
Strategic
Studies

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 1

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 1: Protecting Electoral Infrastructure from Russian Cyberoperations

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 labelling 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

1

Diplomatic Measures in Response to Russian Cyber Operations

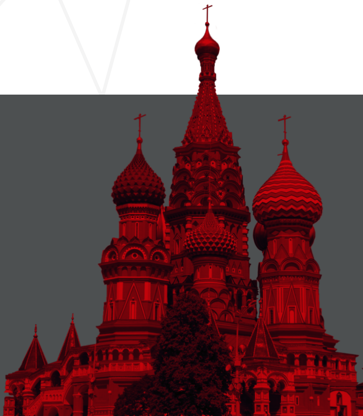
Following Russia’s cyber operations directed against political parties in 2016 (the Macron campaign and the U.S. Democratic Party), alongside international organizations (OPCW), Western governments responded with a series of countermeasures.

Countermeasures	Second-order normative effects
Public attribution and naming & shaming: The highly detailed Dutch attribution following the OPCW hack, in tandem with the previously released details from the Skripal attribution by the U.K., eventually led to a major data breach disclosing the identities of over 300 GRU officers	Highly detailed attribution may set a precedent for and inherently contribute to the Russian narrative that a burden of proof is required by the victim.
Indictments: The U.S. indicted 12 GRU officers for the 2016 presidential election hacking and the OPCW hack. European partners did not join this effort.	Politicizing indictments can escalate lawfare. As a result, states like Russia and China may act more aggressively and freely to politicize international law enforcement as a response.
Sanctions: Whilst the U.S. was quick to enact sanctions against Russia for its actions, the EU and its member states remained reticent to employ similar actions, despite its Cyber Diplomacy Toolbox.	The second order-normative effects of sanctions were not considered in this case.
Diplomatic Expulsions: The U.S. expelled 35 Russian diplomats for the 2016 election interference; a coordinated European response had 19 member states expelling Russian officials.	The second order-normative effects of diplomatic expulsions were not considered in this case.

Norm emergence

Norm prohibiting cyberoperations against electoral infrastructure

The entrepreneurs, initially the GCSC and later the French government (using the Paris Call as organizational platform) and Dutch government (using the UN as organizational platform), framed the norm to threats to democracy and sovereignty, and linked it to the existing norms on non-intervention and critical infrastructure protection.



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 starts by analyzing the diplomatic countermeasures by the U.S. and European governments in response to Russian cyber operations, as part of its larger hybrid campaign aimed at undermining international and democratic institutions and processes. More specifically, the report takes a closer look at the underlying mandate of the countermeasures, their second-order normative effects, and how they led to the emergence of a norm to protect electoral infrastructure. Whilst the norm is in its early stages of the lifecycle, the strategies and tools of influence used by the entrepreneurs can be described as pluralistic, meaning that they intend for the norm to be spread and internalized using multiple tools of influence simultaneously. In its early stages, multiple state and transnational NGO entrepreneurs *persuade* others by *framing* the norm to larger issues such as the threat to democracy and sovereignty from malign state and non-state actors, and by *linking* it to well-established norms on nonintervention and critical infrastructure protection. Linking and framing a norm as an enhanced interpretation of existing norms can be seen as a tactical bargaining tool to persuade like-minded countries that rather focus on implementing previously agreed UN cyber norms over creating new norms. This reinforces the belief that often the best path to support the acceptance of existing norms is to agree on new add-ons to reinforce existing ones. Ultimately, *coercion* occurred through diplomatic expulsions, sanctions, and indictments. *Socialization* tools mainly focused on stigmatizing Russia and promoting the norm with like-minded parties via organizational groups such as the GCSC, Paris Call, and the UN.

This 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

[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.

alternative 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: Protecting Electoral Infrastructure from Russian Cyberoperations

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 European countries toward Russian malicious cyber operations, as part of their larger hybrid campaign aimed at undermining international and democratic institutions and processes. Ultimately, it is shown how these actions by the West led to the emergence of a norm to protect electoral infrastructure from cyber operations.

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 both horizontally 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. To this end, this case study deals with diplomatic and economic countermeasures in response to Russian cyber operations.

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

This case study focuses on the diplomatic countermeasures taken by the U.S. and European governments in response to Russian malicious cyber operations, as part of its larger hybrid campaign aimed at undermining international and democratic institutions and processes. The incident covered by the case study focuses primarily on the documented operations of APT-28 - aka *Fancy Bear* - between 2016 and 2018, which operated as part of Russia's GRU. This includes the hacking of U.S. and European political parties[12] and the attempted intrusion into national and international chemical organizations such as the Organization for the Prohibition of Chemical Weapons (OPCW).[13]

[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%20 the%20Kremlin%20House%20of%20Mirrors.pdf.

[12] Hacking of electoral infrastructure and parties in the U.S. presidential elections from March 2016, primarily directed at the Democratic National Committee (DNC) Clinton's campaign, and subsequently the French elections in 2017, which targeted the Macron campaign. The attack methods centered on spear phishing campaigns to capture user credentials in order to access and subsequently leak confidential documents; overtly monitor the computer activity of dozens of employees; and implant hundreds of malicious files to steal passwords and maintain access to the networks.

[13] Organizations believed to be involved in the investigation of the chemical attack against Sergei Skripal and the use of chemical weapon attacks in Syria were targeted, most notably during the close access GRU operation targeting the Organization for the Prohibition of Chemical Weapons (OPCW) computer networks through Wi-Fi connections in April 2018. The OPCW operation was foiled and reported on by the Dutch Military Intelligence Services.

These operations place Russian doctrines of "active measures" and "reflexive control" within the context of cyberspace, in which strategic operations are planned and executed with psychological effects as the main underlying motivation. Russia's view of the importance of information as a weapon was clarified in the 2016 Information Security Doctrine, in which it distinguished two forms of informational attacks: a technical and a psychological attack.[14] It is mostly concerned with the latter, and nearly all technical attacks (including cyber and electronic attacks) are coordinated or supplemented with a psychological effect in mind. As such, the hacking of the U.S. Democratic National Convention (DNC) and the Clinton and Macron presidential campaigns led to the subsequent leaking of confidential documents, altered with fabricated information, amplified through Russian-aligned media outlets, such as RT and Sputnik, internet trolls, and co-opted sympathetic groups, like Wikileaks. The hack, therefore, allowed Russia to exploit existing societal differences, undermine Western democratic processes, and establish narratives in favor of the Kremlin.

3.2 Countermeasures

Diplomatic and economic responses to Russian cyber operations have alternated across Western countries, including France, the Netherlands, and the United States - ranging from public attribution, indictments to the imposition or threat of sanctions. European countermeasures, both French and Dutch, have remained limited to the lower end of the escalation ladder and include public attribution, naming and shaming, and diplomatic expulsions. This section includes an overview of the countermeasures and their underlying mandate.

3.2.1 Public attribution and naming & shaming:[15]

In October 2016, the U.S. Department of Homeland Security and the Office of the Director of National Intelligence attributed in a general sense the "recent compromises of e-mails from U.S. persons and institutions, including from US political organizations" to Russia.[16] In July 2018, the U.S. government issued a more

[14] Ministry of Foreign Affairs of Russia: "Doctrine of Information Security of the Russian Federation", (2016): https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

[15] Attribution includes both technical and a political components. At the outset, it involves collecting and analyzing evidence from both technical and other intelligence assets. On the basis of the intelligence evaluation, the state will then make the political decision whether or not to communicate – openly or covertly – about the attribution. This strategy is often used to implicitly signal to opponents that one's technical attribution capabilities have improved markedly and have the political willingness to communicate the attribution as a first step, diminishing the margin for plausible deniability for the perpetrator as they are no longer invisible. See the guide to cyber attribution specifying general indicators and examples of successful attribution by Office of the Director of National Intelligence, "A Guide to Cyber Attribution", (September 2018):. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

[16] United States Department of Homeland Security, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security", (2016): https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

detailed account of hacking offenses related to the 2016 election in an indictment against Russian operatives.[17] In response to the Russian-orchestrated 'Macron Leaks' operation, it was easier for French officials to attribute the *disinformation campaign* to Russia because of the overt nature of parallel campaigns orchestrated by Russia Today and Sputnik. However, they never publicly attributed the *hack* to Russia.[18] Finally, the British response to the September 2018 poisoning of Sergei Skripal and subsequent Dutch response to the OPCW operation disclosed a high level of evidence, including identities and personal data of the GRU officers they believed to be responsible.[19] A few days after the Dutch statement, the independent investigative collective Bellingcat, utilizing the published passports and information previously disclosed by the U.K. in response to the Skripal poisoning, exposed a major data breach disclosing the identities of approximately 305 GRU officers.[20] This proactive approach to naming and shaming had concurrent material and operational costs for Russia that neither the U.K. nor the Netherlands may have anticipated. It amounted to one of the few instances where naming and shaming served as an effective imposition of costs against Russia.

Mandate Attribution: In the nation state context, public attribution, whether in the cyber or physical realm, is a political act based on sovereignty, and while there is no particular agreed upon standard of proof, countries still have a strong incentive to not make spurious allegations, lest they lose credibility.[21] Rather than employing collective or joint attribution, the EU's approach is predicated upon the principle that attribution is a political or sovereign decision made by the member states. It can be better described as coordinated among member states through information and intelligence sharing. Finally, it is important to note here that in the legal requirements for countermeasures as set forth by the International Law Commission in its Articles on State Responsibility, which generally reflect customary international law, the "injured" state's countermeasure must be intended to convince the "responsible" state to desist in its unlawful activities.[22] Countermeasures are, thus, subject to strict conditions, including the requirement that the injured state invokes the other state's responsibility. This involves the injured state establishing a violation of an obligation under international law that applies between the injured state and the responsible state and requires that the cyber operation can be **attributed** to the responsible state.[23]

Diplomatic expulsions: Diplomatic expulsions go one step further in imposing costs on the perpetrator. The EU and its member states have made little use of indictments or sanctions in responding to malicious cyber operations thus far. Their use of public attribution contributed to a unified European response resulting in the expulsion of over 100 Russian diplomats by 19 EU member states and 10 other states, including the U.S. in March 2018, in response to the Skripal poisoning and the intended OPCW hack. As a response, the Kremlin escalated the crisis further when they decided to

[17] The United States Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election", (2018): https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

[18] 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.

[19] Odell, Mark, "How Dutch Security Service Caught Alleged Russian Spies", Financial Times (2018): https://www.ft.com/content/b1fb5240-c7db-11e8-ba8f-ee390057b8c9.

[20] Bellingcat Investigation Team, "305 Car Registrations May Point to Massive GRU Security Breach", (2018): https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/.

[21] Global Commission on the Stability of Cyberspace, "Advancing Cyberstability", (2019): https://cyberstability.org/report/.

[22] United Nations, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries", International Law Commission (2008): https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

[23] Ministry of Foreign Affairs of the Netherlands, "Letter to the Parliament on the International Legal Order in Cyberspace", (2019): https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

expel 40 American diplomats and close the American Consulate in St. Petersburg as a response, resulting in a further deterioration of U.S.-Russia relations.[24] Earlier, the U.S. undertook similar measures when it expelled 35 Russian diplomats for alleged interference into the U.S. presidential elections in December 2016.[25] Such a widespread expulsion of Russian diplomats had not occurred since the end of the Cold War. After threatening to retaliate in kind, Moscow eventually decided not to expel any diplomats, most likely because of U.S. presidential transition, which redirected the attention away from the hack while simultaneously offering an olive branch to incoming President Trump.[26]

Mandate Expulsions: A state can expel diplomats when they are considered "persona non grata", as defined under article 9 of the Vienna Convention Diplomatic Relations.[27] In this context, the diplomatic expulsion should be considered an act of *retortion*, an unfriendly but not unlawful measure that a state can take in response a similar act by another state's[28] Countermeasures are defined under international law as measures that would normally constitute a violation of an obligation under international law but which are permitted because they are a response to a previous violation by another state. They are subject to strict legal and political requirements, whereas retorsions can be taken at any time without taking these considerations into account as long as they are in line with their obligations under international law.[29]

Indictments: Within this case study, the U.S. took an assertive approach in its use of indictments. In July 2018, it indicted 12 Russian GRU officers for hacking the 2016 presidential elections - mostly targeting the DCCC and DNC networks, and the subsequent release of stolen documents.[30] It marked the first impactful acknowledgment and response from the Trump administration that a Russian government agency was behind the attack.[31] Following the public attribution of the Russian operatives behind the OPCW operation, the U.S. followed suit with indictments in October 2018, bringing charges against the GRU officers who were, amongst other things, involved in the OPCW operation.[32]

[24] Higgins, Andrew, "Expelling Diplomats, a Furious Kremlin Escalates a Crisis", New York Times (29 March 2018): https://www.nytimes.com/2018/03/29/world/europe/russia-expels-diplomats.html.

[25] Gambino, Lauren; Siddiqui, Sabrina; Walker, Shaun, "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking", The Guardian (2016): https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack.

[26] Tamkin, Emily, "After Russians Promise Retaliation, Putin Decides Not to Expel U.S.", Foreign Policy (30 December, 2016): https://foreignpolicy.com/2016/12/30/after-russians-promise-retaliation-putin-decides-not-to-expel-u-s-diplomats/

[27] Article 9 of the Vienna Convention: "The receiving State may at any time and without having to explain its decision, notify the sending State that the head of the mission or any member of the diplomatic staff of the mission is persona non grata or that any other member of the staff of the mission is not acceptable. In any such case, the sending State shall, as appropriate, either recall the person concerned or terminate his functions with the mission. A person may be declared non grata or not acceptable before arriving in the territory of the receiving State.", United Nations, "Vienna Convention on the Law of Treaties", (23 May, 1969): https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf.

[28] International Law Commission, "Draft articles on responsibility of States for internationally wrongful acts, with commentaries", (2001) Yb ILC vol. II, Part Two.

[29] Ministry of Defense of the Netherlands, "About the Netherlands Law Review", Military Law Magazine (2019): https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/.

[30] United States Department of Justice, "Case 1:18-cr-00215-ABJ Indictment", United States District Court for the District of Columbia, (2018): https://www.justice.gov/file/1080281/download.

[31] Greenberg, Andy, "Trump's Win Signals Open Season for Russia's Political Hackers", WIRED (2016): https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/; https://www.wired.com/2016/11/trumps-win-signals-open-season-russias-political-hackers/.

[32] United States Department of Justice, "U.S. Charges Russian GRU Officers With International Hacking and Related Influence and Disinformation Operations", Office of Public Affairs (2018): https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

When Concord, a Russian company charged by the U.S. Mueller indictment, was the first to contest its charges in March 2020, the New York Times reported that “instead of trying to defend itself, Concord seized on the case to obtain confidential information from prosecutors, then mount a campaign of information warfare, a senior Justice Department official said.”[33] As a result, the U.S. Justice Department dropped the charges to preserve national security interests and prevent Russia from weaponizing lawful protocols to acquire delicate American law enforcement information, according to the official. A guilty verdict against companies that cannot be meaningfully punished in the United States did not measure up against the risk of exposing national security secrets.[34]

Mandate Indictments: Bringing criminal charges in the form of indictments against foreign hackers differs from sanctions, expulsions or even military measures for responding to malicious cyber intrusions for two main reasons. First, criminal charges and indictments are carried out by law enforcement agencies to target individuals, rather than states, for criminal wrongdoing on the basis of domestic legislation.[35] Second, bringing criminal charges requires evidence that meets the requisites of probable cause by a grand jury or a judge in order to bring charges. This is in contrast to public state attributions where there is no evidence threshold and intelligence assessments may use classified sources and methods that may not be admissible in court.[36]

Mandate Sanctions: There is a large existing sanction framework in place at the UN, EU and national level that can be imposed against states, organizations, and persons encompassing financial sanctions (asset freezes), trade embargoes (flight and shipping bans or export limitations), arms embargoes (prohibition of weapon and dual-use exports), and travel restrictions (visa bans). Both within the EU and the U.S. context, sanctions targeting malicious cyber operations are primarily directed at persons or organizations rather than states. In the US, the Treasury Department is the agency and does so based on Executive Order 13757 and 13694 that specifically deal with cyber-enabled activities, as well as pre-existing sanction statutes and regulations.[37] The Russian operatives sanctioned by the U.S. were done pursuant to the Countering America’s Adversaries Through Sanctions Act (CAATSA).[38] The EU endorsed its sanction regime to counter malicious cyber operations in June 2017 through the so-called Cyber Diplomacy Toolbox. [39] It is coordinated by the European External Action Service and includes restrictive measures for individuals and other entities, such as asset freezes and travel bans.

Sanctions: In December 2018, the U.S. Department of the Treasury imposed Russia-related sanctions, adding 18 Russians to their blacklist that were acting for or on behalf of, directly or indirectly, the GRU.[40] Amongst other allegations, they were found to be involved in hacking and meddling in the 2016 U.S. presidential election and against the OPCW. Consequently, any property or interests of these persons, subject to or transiting U.S. jurisdiction were blocked. The EU has thus far only used

[33] Benner, Katie; LaFraniere, Sharon, “Justice Dept. Moves to Drop Charges Against Russian Firms Filed by Mueller”, New York Times, (2020): https://www.nytimes.com/2020/03/16/us/politics/concord-case-russian-interference.html.

[34] *Ibid*.

[35] In the U.S. case, the most cited legal basis for the indictments concerning malicious cyber operations derive from the Computer Fraud and Abuse Act: Doyle, Charles, “Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws”, Congressional Research Service, (15 October, 2014): https://fas.org/sgp/crs/misc/97-1025.pdf; Johnson, Carrie: “U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports And Doping Groups”, NPR (2018): https://www.npr.org/2018/10/04/654306774/russian-cyber-unit-accused-of-attacking-opcw-chemical-weapons-watchdog; United States Department of Justice, “U.S. Charges Russian GRU Officers With International Hacking and Related Influence and Disinformation Operations”, (2018): https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

[36] *Ibid*.

[37] United States Department of the Treasury, “Sanctions Related to Significant Malicious Cyber-Enabled Activities” (2019): https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx.

[38] United States Department of the Treasury, “Treasury Targets Russian Operatives Over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities”, Press Releases (2018): https://home.treasury.gov/news/press-releases/sm577.

[39] Council of the European Union: “Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States” EUR-LEX Document 32019R0796 (2019): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.ENG&toc=OJ:L:2019:129I:TOC.

[40] U.S. Department of the Treasury: “Treasury Targets Russian Operatives Over Election Interference, World Anti-Doping Agecy Hacking, and Other Malign Activities”, Press Releases (2018): https://home.treasury.gov/news/press-releases/sm577 .

its recently acquired Cyber Diplomacy Toolbox once to adopt similar sanctions in response to Russian, Chinese and North Korean hacks, including the attempted hack against the OPCW.[41] Such a decision requires unanimity from all EU member states, which may make its use problematic considering some member states' entanglement with Russia on issues outside of the purview of this case study, such as energy dependencies, which may require them to adopt less coercive measures and seek cooperation and persuasion instead. This trend is indicated in the actions of German-French rapprochement towards Russia despite its information operations against both countries, [42] although increased pressure from the Dutch (and previously the UK) and more recently from the Germans has gone some way toward indicating a willingness to use sanctions against Russia.[43]

In summary, the countermeasures described eliminate the secrecy surrounding cyber operations and may serve to rebalance the cost-benefit calculations of future hybrid aggressors, as their operations illicit economic sanctions and legal indictments which raise the cost of their activity. Additionally, the largescale GRU data breach highlights the effectiveness of attribution as a form of punishment and the risk of unanticipated consequences of hybrid action, where previously they may have been viewed as a low-cost alternative to direct confrontation. The countermeasures employed by the U.S. and EU states reflect differences in capabilities, vulnerabilities, and their overall guiding doctrines in responding to a mutual problem. The constraints of political coordination amongst EU member states to use coercive tools, the relatively young mandate to use them, and mutual dependencies with Russia restrict Europe from embarking on the same coercive measures – such as sanctions and indictments – undertaken by the United States. Alternatively, proactive U.S. countermeasures may be viewed as a means

[41] European Council, "EU Imposes the First Ever Sanctions against Cyber-Attacks", (30 July, 2020): http://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

[42] This aspect of persuasion is principally a Franco-German approach, informed through its interferences with Russia; consequently, President Macron has sought common ground with Russia, featuring Putin at various functions including his summer residence at Bregancon, and was due to attend Russia's 75th Victory Day celebrations. These legitimation overtures followed Russia's readmission to the Council of Europe, the construction of the Germany-Russian Nordstream 2 gas pipeline, reinforcing the narrative of a European rapprochement with Russia via material and political incentives: RFI, "Macron Hosts Putin For Talks in Southern France", (19 August, 2019): http://www.rfi.fr/en/europe/20190819-macron-hosts-putin-talks-southern-france; TASS, "Macron's Visit to Moscow on Victory Day Reflects Approach to Ties With Russia, Says Envoy", (5 February, 2020): https://tass.com/world/1116933; Economist, "A Thaw in EU-Russia Relations is Starting – Undeserved Détente", (12 October, 2019): https://www.economist.com/europe/2019/10/12/a-thaw-in-eu-russia-relations-is-starting.

[43] Nonetheless, the EU has issued travel restrictions and asset freezes for individuals related to the Iranian "Cyber Police" on the basis of human rights violations, followed by embargoes on equipment that may be used to monitor or intercept internet and telephone communications on mobile or fixed networks: Council Implementing Regulation, "Implementing Regulation No 359/2011 Concerning Restrictive Measures Directed Against Certain Persons, Entities and Bodies in View of the Situation in Iran", EUR-LEX (8 April, 2019): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.098.01.0001.01.ENG&toc=OJ:L:2019:098:TOC; Stolton, Samuel, "EU Backs Cyber Sanctions Regime, Following Dutch and UK Pressure", EURACTIV,(17 May, 2019): https://www.euractiv.com/section/cybersecurity/news/eu-backs-cyber-sanctions-regime-following-dutch-and-uk-pressure/.

to compensate for its relatively weak resilience[44], whereas the EU and its member states focus on their relatively better resilience posture supplemented by less coercive countermeasures, such as naming and shaming. [45] These realities inform the preference of methods by which both actors formulate their strategic postures, including the use of countermeasures. The following section extrapolates these measures in terms of their influence over emergent norms, and their second-order impacts upon the wider body of established and internalized norms.

3.3 The Normative Dimension: What Norms are Promoted?

As indicated in the theoretical framework, habit and repetition alone – in particular when they go unchallenged – create norms. The U.S. and European actions were aimed to denounce and break a Russian pattern of behavior that could otherwise establish a norm. These countermeasures are thus primarily intended to reinforce or establish norms and red lines that shape Russian behavior. The normative dimension of this case study first looks at whether the countermeasures reinforce existing norms or if they lead to the emergence of a new norm. Finally, we identify second-order effects that result from the countermeasures that may conflict with the European and American long-term interests and counter-hybrid posture.

3.3.1 Affirmation of Existing Norms?

Despite differences in their escalation posture, one could argue that both the U.S. and European responses indicate a commitment to reaffirm the existing norm prohibiting cyberattacks against critical infrastructure from the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which is broadly adopted by all members of the UN General Assembly. The norm, however, does not specify what constitutes critical infrastructure. While the U.S. and several of its European counterparts may

[44] As noted by Alexander Klimburg, a major reason for the vulnerable state of U.S. cybersecurity is due to its scale: “large nations have inherently more attack surface to cover, and the U.S. easily has the greatest attack surface of them all.” This vulnerability is reflected by the poor state of U.S. cybersecurity at all levels of government (federal, state and local), military weapon systems and critical infrastructure. This does not mean that the U.S. does not undertake protective measures or that European resilience is easy, but informs the underlying reasons that inform their posture. Klimburg, Alexander, “Mixed Signals: A Flawed Approach to cyber Deterrence”, Survival 62 (1) February-March 2020) pp.116-117.

[45] This aspect of persuasion is principally a Franco-German approach, informed through its interferences with Russia; consequently, President Macron has sought common ground with Russia, featuring Putin at various functions including his summer residence at Bregancon, and was due to attend Russia’s 75th Victory Day celebrations. These legitimation overtures followed Russia’s readmission to the Council of Europe, the construction of the Germany-Russian Nordstream 2 gas pipeline, and reinforcing the narrative of a European rapprochement with Russia via material and political incentives. RFI, “Macron Hosts Putin For Talks in Southern France”, (19 August, 2019): http://www.rfi.fr/en/europe/20190819-macron-hosts-putin-talks-southern-france; TASS, “Macron’s Visit to Moscow on Victory Day Reflects Approach to Ties With Russia, Says Envoy”, (5 February, 2020): https://tass.com/world/1116933; Economist, “A Thaw in EU-Russia Relations is Starting – Undeserved Détente”, (12 October, 2019): https://www.economist.com/europe/2019/10/12/a-thaw-in-eu-russia-relations-is-starting.

label electoral infrastructure as critical, Russia may not. While the countermeasures may indirectly link to the respective norm, the commitment remains circumstantial at best and could be improved through specifying the exact norm violations by Russia. Should states decide to *link* to the norm violation in their response, norm adherence and accountability is improved through reaffirmation. If this is not done, countermeasures risk challenging or even violating established norms. This risk is further exacerbated by the U.S. persistent engagement doctrine that allows for a more offensive cyber posture, which is explained in more detail in case study 2. Whilst some might argue that the routine violation of ostensibly internalized norms by states like Russia could undermine these efforts, countries like the U.S. and its European counterparts have worked to build support for its condemnations of their activity amongst allies and other nations. If there is no response regardless, states risk normalizing malicious behavior through tacit acceptance.[46]

3.3.2 A New Norm Emerges?

Alternatively, one could argue that the record of public attributions, indictments, sanctions and diplomatic expulsions contributed to the emergence of a new norm to protect electoral infrastructure from cyber operations. By labeling specific infrastructure such as electoral systems as critical, the norm creates an enhanced interpretation of the GGE norm on the protection of critical infrastructure. Academic research has shown that it can take years for norms to be commonly adhered to and that often the best path to support the acceptance of existing norms is to agree on new add-ons to reinforce existing ones.[47]

Norm Emergence: Framing and Linking

The explicit norm proposal to protect electoral infrastructure originated in 2018 from the Global Commission on the Stability of Cyberspace (GCSC) [48], a transnational civil society-led initiative, and was later adopted by the Paris Call for Trust and Security in Cyberspace – a high-level declaration of French President Macron with over 1,000 state, industry and civil society signatories, but excluding Russia, China and the

[46] The need for norm accountability is aptly described in the final report of the Global Commission on the Stability of Cyberspace: "Even if an aggrieved party is satisfied that a particular actor is responsible (and attribution has in fact occurred in international cases), holding actors truly accountable has also proven challenging, thus undermining the value of norms. After all, if there are no adverse consequences for those who violate accepted norms, those norms become little more than words on paper and they will be unlikely to discourage destabilizing activities," Global Commission on the Stability of Cyberspace, "Advancing Cyberstability – Final Report", (November, 2019): https://cyberstability.org/report/.

[47] Klimburg, Alexander; Almeida, Virgilio, "Cyber Peace and Cyber Stability: Taking the Norm Road to Stability," *IEEE Internet Computing* 23, no. 4 (1 July-Aug. 2019), pp. 61-66.

[48] The GCSC norm on protecting electoral infrastructure states that "State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.": Global Commission on the Stability of Cyberspace, "Advancing Cyberstability – Final Report", (November, 2019): https://cyberstability.org/report/#appendix-b-the-norms-of-the-gcsc; https://pariscall.international/en/principles.

United States.[49] Given that the norm is relatively new, it is best categorized within the early stages of its lifecycle: norm emergence. The main actors in this case are the *norm entrepreneurs* that can create or leverage influence in *organizational platforms* to convince a critical mass of actors to embrace the new norm in its early stages by *framing* it within a particular context that works favorably to the interests of the entrepreneur and by *linking* it to other impactful issues that attract attention and resources.

The entrepreneurs, in this case, initially the GCSC and later the French government (the main actor behind the Paris Call) and Dutch government (advocated for the norm in the UN), *frame* the norm within a particular context, thereby shaping the identity of the players affected by the norm. In contrast to the norms developed within the interstate UN context, this particular norm puts the onus not only on states but also on non-state actors, thereby extending its applicability to proxy actors. In terms of the prescribed behavior, the norm can be considered regulative, prohibiting offensive cyber operations from targeting the technical infrastructure essential to elections, referendums or plebiscites, while it excludes the contentious issue of content or disinformation. Such offensive operations are framed as a threat to democracy by *linking* it to the principle of non-intervention enshrined in article 2(4) of the United Nations Charter, explaining that elections lie at the heart of sovereignty, territorial integrity and political independence.[50] While the norm did not utilize naming and shaming tactics or accused actors explicitly, it was proposed at a timely moment, just after the described incidents of this case, and linked the norm to the growing number and intensity of threats to participative processes, and recognizing that such attacks are unacceptable.[51]

Socialization

Using the Paris Call for Trust and Security in Cyberspace, linked directly to the Paris Peace Forum and indirectly to Internet Governance Forum, as an organizational platform, France managed to *socialize* its emerging norm entrepreneurship within a large group of like-minded countries, as well as industry and civil society. While a large majority may subscribe to the norm because they agree with the content, others may have acted more strategically by adopting the emergent norms to avoid stigmatization without the intention of actually upholding its principles – a form of social camouflage through false-positive. This is especially effective in tight-knit groups, such as EU

[49] The Unites States did not state why it did not sign the accord, but one possible explanation would be that it's a tactical decision wherein the U.S. refuses to adopt new cyber norms, especially outside of the remit of their preferred diplomatic vehicle that is the United Nations Group of Governmental Experts.

[50] Article 2(4) of the UN Charter states: "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": https://www.un.org/en/sections/un-charter/un-charter-full-text/.

[51] Global Commission on the Stability of Cyberspace: "Norms of the GCSC", Advancing Cyberstability, (2019): https://cyberstability.org/report/#appendix-b-the-norms-of-the-gcsc.

member states, wherein they are concerned with their reputations within their specific community. After all, conformity to the Paris Call improves the reputation of a state as a responsible actor as it operates as a public member of its community. This is especially the case when a norm entrepreneur uses organizational platforms to institutionalize the norm. This could in turn contribute to a dynamic of imitation and bandwagoning as norm leaders attempt to socialize other actors to become norm followers. This was reflected by the near threefold growth of total subscribers to the Paris Call, of which state parties grew from just over 50 to 70.[52] When it comes to the effect of socialization in relation to Russia, the tool of influence is limited to *stigmatization* as Russia, along with the U.S. and China, did not sign up for the Paris Call. This stigmatization is enhanced by more coercive socialization tools, such as public attribution or naming and shaming.

Through its active advocacy functions, both the GCSC and the Paris Call acted as organization platforms that created diplomatic momentum and leverage for states, most notably France and the Netherlands, to socialize the norm among state actors within the United Nations Open-Ended Working Group (OEWG) in the Field of Information and Telecommunications in the Context of International Security.[53] It did so by linking it to the pre-existing critical infrastructure as critical; the norm thus creates an enhanced interpretation of the GGE norm on the protection of critical infrastructure.

Persuasion

In terms of persuasion, the norm entrepreneurs used framing techniques in addition to linking the norm to other powerful pre-existing norms to increase its credibility and urgency. While like-minded countries within the OEWG would rather focus on promulgating already established norms, rather than adopt new ones, this norm is *framed* as being an expansion to a pre-existing norm established by the GGE on the protection of critical infrastructure. This *links* the argument to the fact that multiple countries, such as the U.S., have already internalized their norm in national legislation by considering electoral infrastructure as critical and thus requiring merely the extension of existing standards, rather than the formulation of entirely new norms.

In terms of positive inducements or material incentives, there are few overt measures that are directly linked to the promotion of the norm. One exception may be the capacity building partnerships between industry and civil society within the context of

[52] Paris Call, “For Trust and Security in Cyberspace”, (11 November, 2018): https://pariscall.international/en./

[53] Ministry of Foreign Affairs of The Netherlands, “The Netherlands’ Position Paper on the UN Open-ended Working Group “on Developments in the Field of Information and Telecommunications in the Context of International Security” (14, October, 2019); United Nations Group of Governmental Experts , “on Advancing State behavior in cyberspace in the context of international security”, (February 2020): https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf.

the Paris Call created, such as the initiative from Microsoft – the industry partner for the Paris Call - and the Alliance for Securing Democracy partnership to prevent malign interference by foreign actors.

Coercion

The third tool used to promote the norm - *coercive strategies* – reflects the previously described countermeasures adopted by the U.S. and its European counterparts towards Russia. These include the use of *coercive socialization* through naming and shaming by the U.S. in response to the hacking of the DNC. Whereas the French government did not officially attribute the *hack* of the Macron campaign (in contrast to the disinformation campaign that was officially attributed), private cybersecurity companies, such as Trend Micro did attribute the hack to the GRU.[54] Diplomatic expulsions, indictments and sanctions were used by the U.S. in response to the interference of the U.S. presidential elections and the hacking of the DNC. The details of these events are explained in the first section of the case study. The sanctions and indictments were justified on the basis of national U.S. mandates and legislation, showing that the U.S. internalized the norm within its policies. While these measures were directed at imposing costs, they also shape the behavior of Russia by drawing a red line and reaffirming a norm that goes against the targeting of electoral infrastructure.

In conclusion, whilst the norm against cyber operations targeting electoral infrastructure is in its early stages of the lifecycle, the strategies and tools of influence used by the entrepreneurs can be described as pluralistic, meaning that they intend for the norm to be spread and internalized using multiple influence strategies simultaneously – through both words and action. In its early stages, multiple state and transnational NGO entrepreneurs *persuade* others by *framing* the norm to larger issues such as the threat to democracy and sovereignty from malign state and non-state actors, and by *linking* it to well-established norms on non-intervention and critical infrastructure protection. This can be further enhanced through capacity building initiatives and other positive inducements linked to the norm. The entrepreneurs have thus far used organizational platforms such as the GCSC, Paris Call, and the UN, to socialize the norm with both state and non-state actors. While most like-minded countries, such as the US, prefer to focus on implementing previously agreed GGE norms over creating new norms in the UN, the auspicious entrepreneur not only links the norm to these GGE norms but frames it as an enhanced understanding of them. Furthermore, the U.S. diplomatic countermeasures against Russia can be considered an *internalization* of the norm prohibiting cyber operations against electoral infrastructure. The socialization effects of the norm on Russia and China, however,

[54] Perlroth, Nicole, “Russian Hackers Who Targeted Clinton Appear to Target France’s Macron”, New York Times (24, April, 2017): https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html.

is limited to stigmatization, naming and shaming, and more coercive tools, such as sanctions and indictments.

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 countermeasures and the normative initiatives of their opponent. In this case study, we identify three negative externalities associated with the respective countermeasures that are not prohibitive but should be taken into consideration as they have an impact on the development of international norms and could run contrary to the interests of the entrepreneur. These include the effects of attribution on the existing norms or standards of proof and on prohibiting intelligence operations that are not prohibited under international law, and finally the effects of the politicization of indictments on lawfare.

Highly detailed public attribution can set a precedent for a high standard of proof. Although the EU Cyber Diplomacy Toolbox and indictments require an evidence threshold, there is no standard of proof for public attributions by states. Previous public attributions did not disclose a high level of detail regarding the perpetrators, their tools, or the attack vector due to fear of losing intelligence assets. It would provide a glimpse at their operational tools, techniques and methods used to attribute the attack. At the same time, Moscow's rejection of this kind of public attribution is usually based on the lack of evidence provided by the victim state – thereby placing a burden of proof upon the victim at their own cost. This case, however, sets a precedent for highly detailed disclosures that eliminates this plausible deniability of the perpetrator and consequently reveals their techniques, tactics and procedures (TTPs), leading to a more convincing message towards allies and the general public. While this is a largely positive development that does not constitute an explicit effort to establish a new norm on standards of proof, the action and subsequent public attributions of Russia's actions and GRU cyber operations in such recent cases as in Georgia,[55] may inherently contribute to the Russian narrative that a certain burden of proof is required by the victim.

[55] Foreign and Commonwealth Office of the United Kingdom, "UK Condemns Russia's GRU Over Georgia Cyber-Attacks" (20, February, 2020): https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

A lack of clarity about the nature of an incident and the basis of a response can establish a norm against intelligence operations. Aside from the norm setting in terms of *how* states conduct attribution, the response to the OPCW operation reveals something about the kind of behavior it tries to punish. Because offensive cyber operations are preceded by intelligence operations, it remains very difficult to discern the true intention behind an intrusion: is it an intelligence operation, signaling, or preparation of the battlefield? In the Dutch press release following the foiled OPCW hack, the case was considered digital manipulation and sabotage, while others consider it to be an intelligence operation – something that is not explicitly prohibited under international law.[56] If the Russian operation did not violate an international norm or law, is the Dutch response setting a norm against intelligence operations? This remains unlikely, partly due to Dutch self-disclosures about its own security and counter-intelligence operations against the GRU, and partly because it did not take additional further-reaching measures than expelling the Russian operatives. Instead, the GRU officers were indicted by the US. Unless it was contributing to the further blurring between what constitutes acceptable and non-acceptable behavior in cyberspace, the goal of this countermeasure was not to indicate if Russia violated a norm, but to mobilize a broader diplomatic confrontation. As an aspect of the norm lifecycle, this prudence reflects the complications of delineating 'conventional' intelligence operations from the more egregious forms of hybrid meddling perpetrated by Russia. Existing trends amongst victim states show a habit of linking attack vectors to aspects of national security as a means of framing countermeasures; in this way, victim states are demonstrating an effort to define in normative terms the parameters of 'unacceptable' hybrid warfare, as opposed to an accepted form of intelligence gathering.

Politicizing indictments can escalate lawfare. The use of indictments can reinforce existing norms but does not come without risks and possible criticism. Criminal charges are usually processed independently from political considerations. Russia has weaponized this argument by claiming that the U.S. indictments are simply political actions.[57] It hinted at politicization when Concord, a Russian company charged by the U.S. Mueller indictment, was the first to contest its charges in court. In March 2020, The New York Times reported that "instead of trying to defend itself, Concord seized on the case to obtain confidential information from prosecutors, then mount a campaign of information warfare, a senior Justice Department official said." As a result, the Justice Department dropped the charges to preserve national security interests

[56] See Official DISS Statement: "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operations Targeting OPCW", Government of The Netherlands (04 0ctober, 2018): https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw; Smeets, Max, "Does the Dutch Pointing Finger Work in Cyber Attacks?", Clingendael, (10 April, 2019): https://spectator.clingendael.org/nl/publicatie/werkt-de-nederlandse-wijzende-vinger-bij-cyberaanvallen.

[57] Ministry of Foreign Affairs of Russia: "News", (18, June, 2020): https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3294871.

and prevent Russia from weaponizing lawful protocols to acquire delicate American law enforcement information, according to the official This also ties into the broader concern of Western countries about the politicization of international law enforcement efforts and initiatives - a form of lawfare by countries like Russia and China.[58] These adversaries may therefore act more aggressively and freely to politicize international law enforcement as a response and in an effort to undermine cooperation on common issues unaffiliated with inter-state hybrid warfare (i.e. combatting cybercrime). As a reflection of norm development, an increase in lawfare between states through international institutions would significantly challenge norms on multilateral cooperation in cyberspace.[59]

When undertaking countermeasures, states should be aware of the second-order normative effects that can result from their actions. While not insignificant, the effects stemming from diplomatic countermeasures are, and have been, relatively easy to manage and avoid, especially in comparison to those resulting from military or kinetic countermeasures described in the next case study.

3.4 Key Takeaways

Norm entrepreneurs should take advantage of the wider spectrum of tools of influence. The countermeasures described in the first section form the context to which the emergence of a new norm that prohibits cyber operations against electoral infrastructure was linked. The entrepreneurs use multiple strategies and tools of influence to promote the norm – a testament to its pluralistic nature. By pursuing a norm against the hacking of electoral infrastructure, the norm entrepreneurs sought to *persuade* its allies and other actors of the costs these operations impose upon their democratic process and by linking and framing it to pre-existing norms. Additionally, coercion of Russia via diplomatic expulsions, sanctions and indictments, and socialization of the norm with like-minded parties via organizational groups such as the GCSC, Paris Call, and the UN, coupled to further the norm alongside coercive socialization measures to stigmatize Russia via naming and shaming.

The norm moves from emergence to cascade and internalization. Taking into consideration its short lifespan, the norm has already cascaded to a high degree of parties through organizational platforms, and is already being internalized as states,

[58] Gouré, Dan: "How Russia Conducts 'Lawfare': The Case of Interpol", RealClear Defense (31, October, 2019): https://www.realcleardefense.com/articles/2019/10/31/how_russia_conducts_lawfare_the_case_of_interpol_114826.html.

[59] Ruhl, Christian; Hollis, Duncan; Hoffman, Wyatt; Maurer, Tim: "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads", Carnegie Endowment (26, February, 2020): https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

especially powerful norm leaders like the U.S., are categorizing electoral infrastructure as part of their critical infrastructure and take coercive measures to enforce the norm. For now, the socialization effects of the norm on Russia and China, however, is limited to stigmatization, naming and shaming, and more coercive tools, such as sanctions and indictments, which are harder to combine with the other tools of influence. As of now, the norm is included in the pre-draft report of the UN OEWG.[60] Adoption within the UN would constitute a major socialization effect across states, moving beyond norm cascade, and intensifying the internalization process. One could argue that Russia's commitment to the norm is insincere, but it then faces a choice between doubling down on hypocrisy or shifting its behavior in accordance with the norm. Positive inducements, such as capacity building, can be used to accelerate internalization of the norm, and coercive methods can be used to punish transgressors.

States should be aware of the normative second-order effects of attribution and indictments. Norm-setting by countermeasures can have unintended second-order effects, where a state creates a new norm through its countermeasure that may not be in its own strategic interest. Detailed disclosures of evidence in public attributions, whilst good for transparency and eliminating plausible deniability, may be grist to the mill of the Russian narrative that wishes to introduce a standard of proof for public attributions by states. The perceived politicization of indictments may have the same second-order effect on lawfare between states, thereby undermining the norms and rules tied to these platforms as they become embroiled in lawfare. By obfuscating between intelligence and cyberattack operations, a state may also contribute to the further blurring between what constitutes acceptable and non-acceptable behavior in cyberspace. Consequently, intelligence agencies may assume the role of norm entrepreneurs – setting the standards of tolerable conduct in cyberspace for the rest of the international community whilst remaining under the radar of international regulation as sub-state actors.[61] The risks of these normative second-order effects can, and have been, to a large extent mitigated through clear diplomatic engagement. This is not the case for the effects resulting from further-reaching military or kinetic countermeasures described in the next case study.

[60] UN Open-ended Working Group, "Initial "Pre-Draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security", (2019): https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.

[61] Georgieva, Ilina: "The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace", Contemporary Security Policy 41, no. 1, (2019), pp. 33-54: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677389.

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