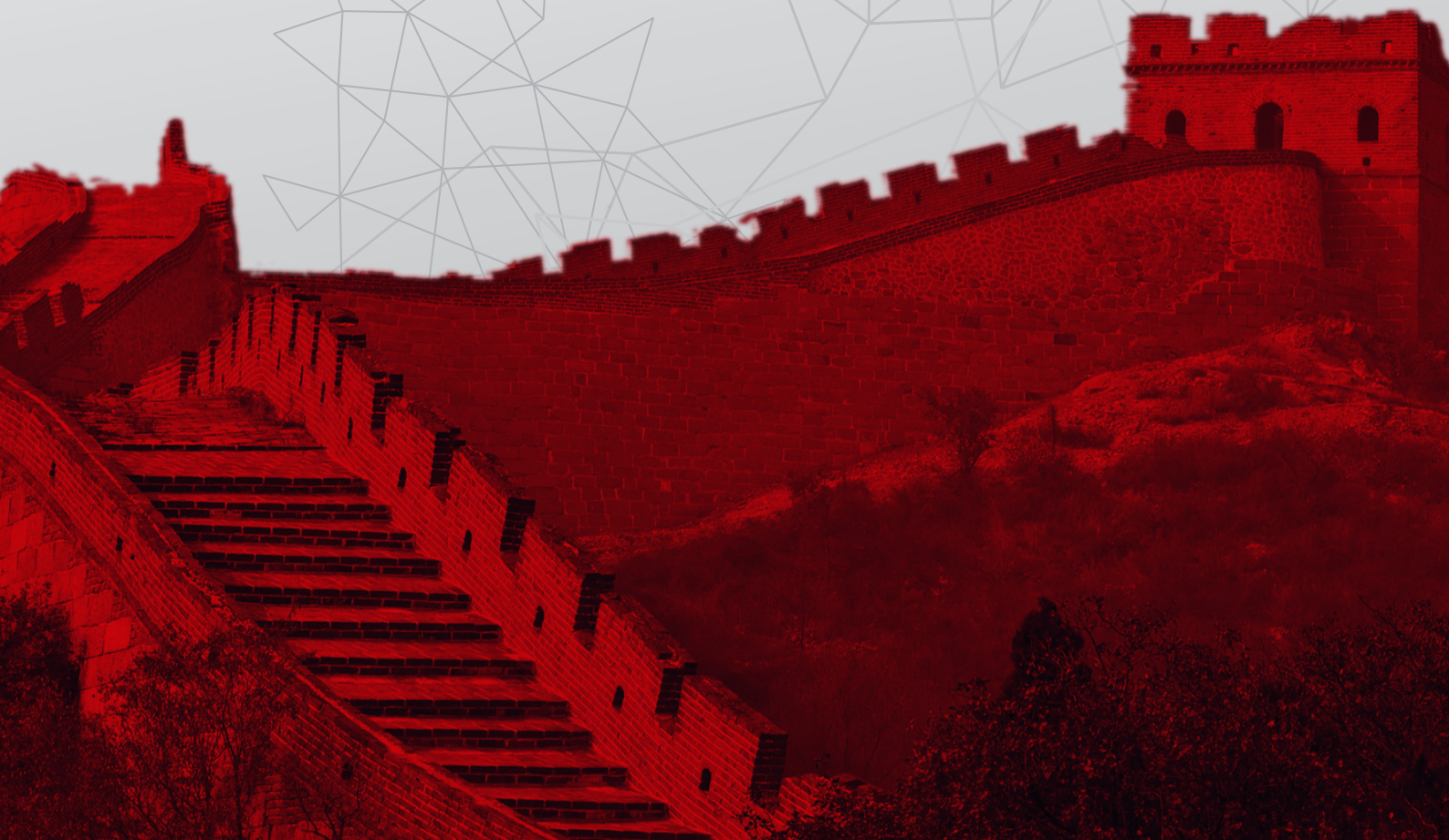
The Hague Centre for Strategic Studies

HCSS PAPER SERIES – CASE STUDY 4

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 4: Responding to Chinese Economic Espionage



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 4

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 4: Responding to Chinese Economic Espionage

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

4

Responding to Chinese Economic Espionage

Several Western companies and states have suffered from a prolonged trend of Chinese cyber-enabled intellectual property theft. After a significant decrease in Chinese cyber espionage following the 2015 U.S.-China agreement, it resurged as bilateral relations soured.

Countermeasures

Sanctions: The Obama administration combined the threat of sanctions with the application of import/export controls and access restrictions to pressure China to acquiesce.

Second-order normative effects

The Trump administration's sweeping trade and tariff war, isolated the norm violation and threat of IP theft as a bilateral issue. It may lead Chinese policymakers to believe they have little to gain from honoring the agreement.

Indictments: The U.S. indicted five Chinese military hackers, marking their intentions in counter-economic espionage enforcement. More indictments also came before and after the 2015 agreement.

Politicizing indictments can escalate lawfare – something that China and Russia are often accused of. They may therefore act more aggressively and freely to politicize international law enforcement as a response.

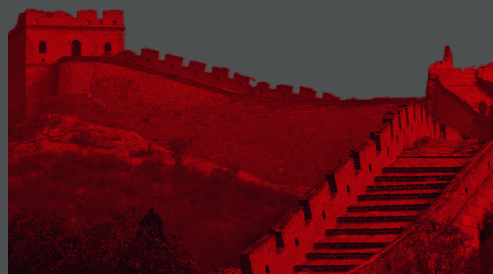
Bilateral Agreement: China and the US produced a Memorandum of Understanding (MOU) in 2015, which agreed upon a prohibition of cyber-enabled IP theft. After a significant decrease, Chinese economic espionage resurged as bilateral relations soured.

The subsequent break with the agreement signals that although Beijing briefly changed its behavior, it may not have done so in the manner Washington promoted in differentiating between 'acceptable' and 'unacceptable' forms of espionage.

Norm emergence

Norm prohibiting cyber-enabled intellectual property theft

The U.S.-China agreement introduced a norm against cyber-enabled intellectual property theft for economic benefits. The US sought to *persuade* China by promising better bilateral ties and its partners by linking the costs of IP theft to its economy and national security, whilst *framing* it in such a way that it would allow conventional political-military espionage operations. It *coerced* China to adopt the norm through indictments and the threat of sanctions, and *socialize* the norm by using the G20 as a platform.



1. Introduction

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

This paper analyzes the diplomatic, economic, and legal countermeasures from the U.S. and several of its allies in response to Chinese economic espionage. More specifically, it 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 prohibit cyber-enabled intellectual property (IP) theft.

American indictments and the threat of sanctions, as well as persuasion tactics, (the promise of better Sino-American relations) showed promising initial results of Chinese internalization of the emerging norm against economic espionage as it led to the most significant, albeit short-lived, reported drop in Chinese IP theft. If we consider the resurgence of Chinese IP theft as a result of the souring of U.S.-China relations under the Trump administration, we can conclude that the persuasive incentives taken by the U.S. to push towards Chinese adherence and internalization have disappeared. Simultaneously, the U.S. changed its coercion strategy away from targeting specific norm violators and towards a broader bilateral trade and tariff war. Chinese policymakers now have little to gain from continuing to honor the norm as bilateral relations worsen regardless of adherence. Furthermore, the sweeping sanctions against China, in combination with the tariffs the U.S. levies on its partners,

isolates the norm violation and the threat of IP theft as a bilateral U.S.-China issue. Instead, the development of the norm may be better served if the U.S. were to mobilize large-scale, coordinated attribution and subsequent sanctions *with* its partners – other victims that have struck similar norms with China, such as Canada, Australia, the UK, or Germany – in the same coordinated fashion as the countermeasures adopted against Russian hacking of democratic institutions. While China may initially have appeared to adhere to the norm, this was not because of its content but rather as part of tactical bargains that serve their interests. Regardless, there is a chance norm internalization or compliance may still become routinized as habits take hold. China may become entrapped by the reciprocal consequences of insincere prior rhetorical commitments in ways that push towards norm conformity and potential acceptance. The alternative is the danger of appearing hypocritical, which would come with reputational and credibility costs.

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

2. Norms Primer

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

2.1 What is a Norm?

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

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

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

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

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

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

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

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

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

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

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

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

2.2 The Norm Lifecycle

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

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

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

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

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.

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

2.3 Tools of Influence

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

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

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

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

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

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

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

3. Case Study: Responding to Chinese Economic Espionage

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 partner countries toward Chinese economic espionage, and how they led to the emergence of a norm prohibiting cyber-enabled intellectual property (IP) theft.

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 Chinese 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 Chinese actions, followed by the Western countermeasures and their underlying mandate. Herein, we use a broader interpretation of countermeasures than the strictly legal definition. Countermeasures encompass the broad range of state responses taken horizontally 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

11 Jong, de Sijbren; Sweijs, Tim; Kertysova, Katarina; Bos, Roel, "Inside the Kremlin House of Mirrors", The Hague Centre for Strategic Studies, (17 December, 2017), p. 9: https://hcss.nl/sites/default/files/files/reports/Inside%20the%20Kremlin%20House%20of%20Mirrors.pdf.

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 Chinese economic espionage.

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 countermeasures taken primarily by the U.S. and to a lesser extent its Western partners, in response to Chinese cyber-enabled intellectual property theft for commercial gain. The theft occurred before the U.S. and China reached agreement on a norm in September 2015 prohibiting such actions, as well as the subsequent period. Assessing and measuring espionage trends and impact is rather challenging given its clandestine nature. Yet, many agreed that there was a noticeable drop in Chinese economic espionage targeting the U.S. in the year following the agreement, albeit with disagreement regarding the underlying reasons for the decrease and explanations as to why and how it resurged from 2017 onwards.

Several Western states and cybersecurity companies – predominantly American – have exposed IP theft campaigns that were carried out by Advanced Persistent Threat (APT) actors affiliated with or coordinated by the Chinese Ministry of State Security (MSS), including APT 10 who is known to target aerospace, telecommunications and government sectors;[12] APT26 who has previously targeted multiple foreign

12 Lo, Kinling. "APT10: What do we Know About the Alleged Chinese Hacking Group?", South China Morning Post (21 December, 2018): https://www.scmp.com/news/china/diplomacy/article/2179107/apt10-what-do-we-know-about-alleged-chinese-hacking-group.

manufacturers of the C919 passenger aircraft;[13] APT3 who stole "files containing commercial business documents" and secret trade data related to GPS, energy and transportation technologies from large US companies".[14] While these operations served economic interests, other cases, such as the Chinese intrusion of Lockheed Martin's networks for F-35 jet technology, served military or national security interests. In other words, they are part of conventional state intelligence operations that not illegal under international law.[15] This entails that this case study will predominantly focus on IP theft for commercial gain, but also illustrates the underlying intentions or motivations for such an operation can and often do overlap, presenting legal or political friction. Thus, the question posed is whether such theft was done as part of an intelligence operation for political-military reasons - and therefore not wholly illegal outside of the scope of international - or an illicit instance of IP theft?

China uses a comprehensive range of economic espionage methods and techniques - encompassing cyber-enabled intrusions to corrupting trusted insiders – in order to improve its competitive edge and its position as an economic and technological leader.[16] Chinese Intellectual Property theft can be contextualized as being one illicit element of a broader state-driven industrial policy (i.e. the industrial policy program *Made in China 2025*) designed to restructure the drivers of modern Chinese economic growth.[17] Aligned with its industrial policy programs, the Chinese predominantly target high-tech, telecommunications, pharmaceuticals, energy and aviation sectors, and the defense industrial base of South and Southeast Asia, Japan, Taiwan, Hong Kong, South Korea, Europe and the United States.[18] Corporate and technological IP theft provides an innovation injection to alleviate reliance upon foreign technologies and supply chains, and thereby are perceived as being integral for the regime's self-reliance and broader survivability goals, national security and, by extension, protection from foreign interference.[19]

---

13 Kurtz, George: "We Stop. So You Can Go.", Crowdstrike (18 June, 2020): https://www.crowdstrike.com/blog/huge-fan-of-your-work-part-1/.

14 Bozhkov, Nikolay. "China's Cyber Diplomacy: A Primer", EU Cyber Direct (2020), p.6.: https://eucyberdirect.eu/wp-content/uploads/2020/03/bozhkov-digital-dialogue-final.pdf.

15 Wall Street Journal, "China's Cyber-Theft Jet Fighter", Wall Street Journal (12 November, 2014): https://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777.

16 Office of the United States Trade Representative, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974", (22 March, 2018): https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

17 Committee on Small Business and Entrepreneurship - United States Senate: "Made in China 2025 and the Future of American Industry", (27 February, 2019): https://www.govinfo.gov/content/pkg/CHRG-116shrg35699/pdf/CHRG-116shrg35699.pdf. Other tools for acquiring technology include S&T investments, talent recruitment programs, academic collaborations, research partnerships, joint ventures, front companies, mergers & acquisitions, as well as legal their legal and regulatory measures; Cimpanu, Catalin : "FBI is Investigating More Than 1,000 Cases of Chinese Theft of US Technology", ZD Net (9 February, 2020): https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/.

18 Seaman, John; Huotari, Mikko; Otero-Iglesias, Miguel: "Chinese Investment in Europe – A Country-Level Approach", European Network Think-Tank on China, (2017): https://www.clingendael.org/sites/default/files/2017-12/ETNC_Report_2017.PDF.

19 The Office of the United States Trade Representative, "Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfers, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974. Section 301 of the US Trade Act of 1974", (27 March 2018), pp. 1-215: https://ustr.gov/about-us/policy-offices/press-office/pressreleases/2018/march/section-301-report-chinas-acts.

3.2 Countermeasures

The increased extent of Chinese economic espionage has motivated the U.S. to respond through a range of measures including the indictment of specific Chinese cyber actors and companies to the threat of sanctions. Cumulatively, this initial response created sufficient leverage for bilateral negotiations to mitigate reciprocal escalation through the establishment of a Memorandum of Understanding. However, the value of these negotiations, and the role of sanctions and indictments as a motivator, are disputed.

Indictments: The May 2014 indictment of five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization marked an evolution in US' counter-economic espionage strategy - the effectiveness of which has been produced mixed results. The use of indictments continued after the U.S.-China agreement; in November 2017, the Justice Department indicted three Chinese nationals employed by the Chinese cybersecurity firm Boyusec, charging them with hacking into the computer systems of Moody's Analytics, Siemens AG, and Trimble Inc. "for the purpose of commercial advantage and private financial gain."[20] The 2018 indictment of Zhu Hua and Zhang Shilong,[21] two of five Chinese People Liberation Army (PLA) operatives within APT 10, along with the other countermeasures (specifically the bilateral agreement described below) led to a lapse in PLA economic espionage for a limited time. Despite the typical unenforceability of enacting criminal measures against indicted persons, the use of such legal instruments serves a purpose in lending credence to the U.S. and European ability to more robustly identify specific PLA operatives. This way they can link them to identified APTs and tie them to Chinese economic espionage efforts both as violations of established international law and norms. According to U.S. Attorney General William Barr, the U.S. will continue to issue indictments and prosecutions, which coincide with a statement from FBI Director Christopher Wray saying there are about a thousand investigations involving China's attempted theft of U.S.-based technology.[22]

***Mandate Indictments*:** The legal basis for indictments of the Chinese operatives derives from the Economic Espionage Act (1996) and subsequent amendments through the Defend Trade Secrets Act (2016). Specifically, it outlaws: "economic espionage" (18 U.S. Code § 1831), and "theft of trade secrets" (18 U.S. Code § 1832). Section 1832 requires that the thief is aware that the misappropriation will injure the secret's owner to the benefit of someone else, while section 1831 requires only that the thief intends to benefit a foreign government or one of its instrumentalities. In addition, most of the indictments also include charges for "fraud and related activity in connection with computers" (18 U.S.C. § 1030).[23]

20 United States Department of Justice, "United States District Court for the Western District of Pennsylvania – Indictment" (13 September, 2017): https://www.justice.gov/opa/press-release/file/1013866/download.

21 United States Department of Justice, "United States District Court Southern District of New York – Indictment" (17 December, 2018): https://www.justice.gov/opa/press-release/file/1121706/download https://www.justice.gov/opa/press-release/file/1121706/download.

22 Cimpanu, Catalin, "FBI is Investigating More Than 1,000 Cases of Chinese Theft of US Technology", ZD Net,(9 February, 2020): https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/.

23 Doyle, Charles, "Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act", Congressional Research Service (19 August, 2016): https://fas.org/sgp/crs/secrecy/R42681.pdf.

***Mandate Sanctions*:** The existing framework for sanctions within the UN, EU, and U.S. that can be utilized against state and non-state entities is well established and described in detail in Case 1. They encompass a spectrum of measures including individual financial sanctions (asset freezes), trade embargos (flight and shipping bans or export limitations), arms embargoes (prohibition of weapon and dual-use exports), and travel restrictions (visa bans). In the summer of 2015, reports indicated the Obama administration was prepared to use Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," as amended by Executive Order 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities".[27] Furthermore, article 30 of the World Trade Organization's Trade-Related Aspects of Intellectual Property Rights (TRIPS) deals with the protection of undisclosed information.[28] Within the European context, the EU Diplomatic Toolbox can be used to sanction cyber-enabled intellectual property theft.[29]

Sanctions*:* In August 2015, the Obama administration announced it was developing "a package of unprecedented economic sanctions against Chinese companies and individuals" for IP theft.[24] Furthermore, export and import controls and access restrictions were employed in the use of respective technologies by U.S. or Chinese companies.[25] This together with the indictments have increasingly framed bilateral Sino-American relations and acted as momentum for a landmark deal that was reached between then-president Barack Obama and Chinese President Xi Jinping introducing a norm that prohibits IP theft for the benefit of their national economy.[26]

The synchronization between the U.S. with European efforts has not materialized to the extent that it has with other malign cyber actors, particularly Russia. European countries have largely restricted themselves to non-binding protests of Chinese IP theft and diplomatic engagement with Beijing to discuss its cyber theft. Furthermore, U.S. tariffs directed at Europe also delivered a blow at transatlantic relations and the willingness or momentum to coordinate and synchronize efforts with the Europeans. To the degree U.S. sanctions regimes have been upheld by Europe, the multilateral effort has deviated across specific countries and lacks robust coordinated action.

Bilateral agreement: From 2013 to 2015 diplomatic (track 1 and 2) exchanges between China and the U.S. took place on various levels, which together with the coercive

24 Goldsmith, Jack: "More Harmful Public Hand-Wringing on Possible Sanctions Against China for Cyber Theft", Lawfare (31 August, 2015): https://www.lawfareblog.com/more-harmful-public-hand-wringing-possible-sanctions-against-china-cyber-theft.

25 Industry and Security Bureau: "Review of Controls for Certain Emerging Technologies", Federal Register (19 November, 2018): https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

26 FireEye: "RedLine Drawn: China Recalculates its Use of Cyber Espionage", FireEye ISight Intelligence (June 2016): https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

27 The text of the original Executive Order 13694 may be retrieved here: Department of the Treasury, "Sanctions Related to Significant Malicious Cyber-Enabled Activities", Office of Foreign Assets Control (2020): https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx. The amendments in Executive Order 13757 may be retrieved here: United States Department of the Treasury. "Executive Order 13757: Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." Presidential Documents, (28 December, 2016): https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf. The President has extended to April 1, 2019 the national emergency declared in Executive Order 13694 as amended: The White House, "Continuation of the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (27 March, 2018).

28 World Trade Organization, "Intellectual Property (TRIPS) - Part II — Standards concerning the availability, scope and use of Intellectual Property Rights." (2020): https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm.

29 IP theft is included in the definition of 'data interference', which on its turn is one of the actions that can constitute a cyber-attack that could trigger EU sanctions: Council of the European Union, "Legislative Acts and Other Instruments", (14 May 2019): http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf. The EU also has a directive in force "on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure" for members to develop and implement civil protections for trade secrets: European Parliament; Council of the European Union, "Directive 2016/943", (2016): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0943.

countermeasures culminated in a Memorandum of Understanding (MOU) introducing an agreement that prohibited cyber-enabled IP theft for the benefit of their respective national economies.[30] In most of the writing about this case, this bilateral agreement is described as introducing a norm; whilst this train of thought is reflected here, it should be noted that a MOU is not a norm *per se* - it is more politically binding. This case is particularly pertinent because the agreement derived from a norm proposal that the U.S. tried and failed to get signed in the 2015 United Nations Group of Governmental Experts. China suffered from not signing this norm within the UN context and got pushed towards agreement on a more politically binding MOU.

The initial bilateral U.S.-China agreement was met with skepticism and mixed reporting, but the consensus is that it resulted in a significant decline in Chinese-attributed intellectual property theft in the following year.[31] This decline was the highest measurable result decline in IP theft as a result of any U.S. countermeasures to date, so its effects should not be underestimated. However, the results were short-lived as Chinese cyber-enabled IP theft returned, albeit in a lower intensity and higher sophistication.[32]

Alternatively, the short period of decline may be attributed to internal Chinese developments. The drop coincided with major structural reforms (i.e. purges) of the Chinese PLA by President Xi that as a result relocated part of the PLA activities, including espionage, to the Ministry of State Security (MSS).[33] After this transition period, the revival of espionage was considered by some to be more sophisticated and targeted, rather than the noisy bulk collection that had previously been conducted.[34] In Europe, the decline has also been linked to a sharp increase in Chinese foreign direct investment and mergers and acquisitions in high-tech and advanced manufacturing industries in 2016.[35]

Ultimately, the resurgent increase in IP theft may be best explained in terms of the deteriorating Sino-American ties after the Trump administration took office, eliminating any incentives that the Chinese had towards adhering to the norm.[36] The resumption

30 The White House, "Fact Sheet: President Xi Jingping's State Visit to the United States", Office of the Press Secretary (25 September, 2015): https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

31 FireEye: "Redline Drawn: China Recalculates its Use of Cyber Espionage", ISight Intelligence (June 2016): https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

32 Harold, Scott Warren; Libicki, Martin; Cevallosl Stuth, Astrid, "Getting to Yes with China in Cyberspace", RAND (April 2016): https://www.atlcom.nl/upload/RAND_RR1335.pdf vii-viii.

33 Grossman, Derek & Chase, Michael, "Xi's Purge of the Military Prepares the Chinese Army for Confrontation" (April 2016), RAND: https://www.rand.org/blog/2016/04/xis-purge-of-the-military-prepares-the-chinese-army.html.

34 Segal, Adam; Hoffman, Samantha; Hanson, Fergus; Uren, Tom, "Hacking for Ca$h", ASPI (2018): https://www.aspi.org.au/report/hacking-cash.

35 The head of the BfV, Hans-Georg Maassen, linked the decline to the use of legal tools for obtaining the same information, such as corporate takeovers: "industrial espionage is no longer necessary if one can simply take advantage of liberal economic regulations to buy companies and then disembowel them or cannibalize them to gain access to their know-how". *Ibid.*

36 IISS Press Release, "Deterioration in US-China Relations "Deepened and Accelerated' During Trump's Presidency, IISS Dossier Finds", (5 June, 2020): https://www.iiss.org/press/2020/asia-pacific-regional-security-assessment-2020.

of economic espionage led to condemnation from the Five Eyes member countries alongside Japan, Norway, the Netherlands, Germany and Poland.[37] The U.S. has since raised the issue mostly in the context of a larger critique of Beijing's industrial policy and failure to protect IP. It has utilized economic sanctions, including export and import controls and access restrictions to the use of respective technologies by U.S. or Chinese companies.[38] In 2020, the U.S. continued its proactive measures against PLA members citing economic espionage in the Equifax hack aligned with the indictments from the U.S. Justice Department that it had credible attribution means to identify Chinese espionage, which would no longer go undetected.[39] These measures sought to provide freedom for other U.S. departments to leverage cumulative sanctions on Chinese commercial firms, restrictions upon Chinese firms' access to critical supply components, and the imposition of export licensing requirements by the U.S. Department of Commerce.[40] The Trump administration further restricted Chinese investments in particular sectors.[41]

In summary, U.S. countermeasures have principally sought to shape Chinese behavior through imposed costs and diplomatic enticement. Acknowledging its comparatively large attack surface area and valuable IP base, the U.S. has preferred coercive countermeasures to compensate for its relatively weak resilience. In contrast, the EU and its member states – having a relatively young cyber sanction mandate and more difficulty coordinating similar coercive measures – have opted to focus on resilience supplemented by less coercive countermeasures. At the same time, Chinese IP theft seems to be a more salient issue to the U.S. than its European counterparts, that, with the exception of Germany, have relatively less commercially attractive IP. Ultimately, the U.S. countermeasures produced the most impactful curbing effect on Chinese cyber-enabled IP theft to date. As Sino-American relations soured, Chinese incentives to adhere to norm diminished and IP theft resurged. Rather than synchronize its countermeasures with its allies, the U.S. decided to impose tariffs against European

37 Nakashima, Ellen; Lynch, David, "U.S. Charges Chinese Hackers in Alleged Theft of Vast Trove of Confidential Data in 12 Countries", Washington Post (21 December, 2018): https://www.washingtonpost.com/world/national-security/us-and-more-than-a-dozen-allies-to-condemn-china-for-economic-espionage/2018/12/20/cdfd0338-0455-11e9-b5df-5d3874f1ac36_story.html.

38 Industry and Security Bureau, "Review of Controls for Certain Emerging Technologies", Federal Register (19 November, 2018): https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies. McCabe, David, "Huawei Funds Are Cur Off by F.C.C. Over Security Threats", New York Times (22 November, 2019): https://www.nytimes.com/2019/11/22/technology/huawei-funds-cut-fcc.html; United States Office of Public Affairs, "Chinese Military Personnel Charged With Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax", United States Department of Justice, (10 February, 2020): https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

39 *Ibid.*

40 United States Office of Public Affairs, "Fact Sheet: Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", United States Department of Justice (1 April, 2015): https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/fact-sheet-executive-order-blocking-property-certain-persons-engaging-si; Nakashima, Ellen: "U.S. Developing Sanctions Against China Over Cyberthefts", Washington Post (30 August, 2015): https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

41 Lasksai, Lorand, "A New Old Threat", Council on Foreign Relations (06 December, 2018): https://www.cfr.org/report/threat-chinese-espionage.

states, thereby weakening transatlantic relations. The U.S. has stepped towards more aggressive in-band responses in line with its new doctrine on persistent engagement.[42] With this in mind, the following section outlines the normative dimension of these trends and the roles of the respective actors.

3.3 The Normative Dimension: What Norms are Promoted?

The U.S. countermeasures were aimed at setting a red line that breaks the Chinese pattern of behavior that could otherwise establish a norm for economic espionage. At the same time, the countermeasures themselves led to and reinforced the propagation of a norm of acceptable behavior that prohibited cyber-enabled IP theft. This section provides an overview of the normative developments in relation to these countermeasures. Here, we ask if these countermeasures reinforce existing norms or lead to the emergence of a new norm and what, if any, second-order effects arise from the countermeasures.

3.3.1 A New Norm Emerges?

When it comes to espionage, by design, international law does not apply. There are no international legal commitments with regard to not spying, as states do not want formal international constraints on their intelligence agencies. While there may be implicit norms that guide espionage, they are few in number, flexible, and opaque. Despite national law prohibiting IP theft, the U.S. countermeasures and the Obama-Xi agreement are better described as introducing a first international norm against economic espionage, which specifically focuses on the cyber-enabled theft of intellectual property for economic benefits.

Norm Emergence: Framing and Linking

The norm from the 2015 China-U.S. agreement states that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[43] The main antagonists in the first phase of the norm lifecycle are the *norm entrepreneurs* (primarily the U.S.) that identify the G20 as an *organizational platform* to convince a critical mass of actors to embrace the new norm by *framing* the norm within the context of commercial gains and by *linking* it to economic and national security.

---

42 Miller, James; Pollard, Neal, "Persistent Engagement, Agreed Competition and Deterrence in Cyberspace," (April 30, 2019): https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace; Klimburg, Alexander. "Mixed Signals: A Flawed Approach to Cyber Deterrence." Survival 62, no. 1 (March 2020), pp. 116–17.

43 United States Office of the Press Secretary, "Fact Sheet: President Xi Jinping's State Visit to the United States", United States Department of Justice (25 September, 2015): https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

In terms of *framing*, the U.S. limited the norm to cyber-enabled IP theft for *economic benefits*. This excludes other forms of espionage that are conducted for national security benefits. After all, it is not in the U.S. interest to construct a norm that would constrain their intelligence operations within their own national security context. The underlying hope was to get China to accept a distinction between legitimate traditional espionage for political-military ends and illegal espionage for commercial ends.[44]

The U.S. *linked* the norm to the threat it poses to innovation, economic development, and national security, with China identified as the main perpetrator.[45] The norm did not emerge in a vacuum, rather, it has been the result of a longer process. The 2003 U.S. National Strategy to Secure Cyberspace mentioned IP, although it was not a central component of cybersecurity in the 9/11 aftermath. Its importance was raised in the CSIS "Report to the 44th President of the United States on Cybersecurity", where IP protection is not only considered crucial for economic interests but also deemed as important for national security. [46] The Obama administration's "International Strategy for Cyberspace" (2011) included theft of intellectual property as a threat to national security that "threatens national competitiveness and the innovation that drives it".[47] Subsequent government national security and intelligence assessments strengthen this claim further by significantly expanding the definition of IP or trade secrets, *framing* it as a national security issue, identifying China as the main perpetrator, and using it as a rallying cry for better national cybersecurity. Besides the U.S., countries such as Australia,[48] Germany,[49]

---

44 Segal, Adam; Hoffman, Samantha; Hanson, Fergus; Uren, Tom, "Hacking for Ca$h", ASPI (2018): https://www.aspi.org.au/report/hacking-cash.

45 The White House, "International Strategy for Cyberspace" (May 2011): https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

46 The relevant paragraph on IP theft reads: "Most companies' business plans involve the use of cyberspace to deliver services, manage supply chains, or interact with customers. Equally important, intellectual property is now stored in digital form, easily accessible to rivals. Weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign competitors. In the new global competition, where economic strength and technological leadership are as important to national power as military force, failing to secure cyberspace puts us at a disadvantage.", Langevin, J., M.; McCaul, S. Charney; Raduege, H, "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency", Center for Strategic and International Studies (2008).

47 White House, "International Strategy for Cyberspace", (May 2011): https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

48 In its 2016 Cyber Security Strategy, Australia linked IP theft to its security, but it did not explicitly mention China, see Government of Australia, "Australia Cyber Security Strategy 2020", (6 August 2020), p.42: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. In spite of the bilateral agreement, Australians suspect the continuation of Chinese IP theft in recent years, especially after the hacking of National Security University in 2018, which might have led to the theft of sensitive security related data, see McKenzie, Nick; Wroe, David, "Chinese Hackers Put National Security at Risk after Breach.", Sydney Morning Herald (6 July, 2018): https://www.smh.com.au/politics/federal/chinese-hackers-breach-anu-putting-national-security-at-risk-20180706-p4zq0q.html; Department of Foreign Affairs and Trade of Australia, "Attribution of Chinese Cyber-Enabled Commerical Intellectual Property Theft", (21 December, 2018): https://www.dfat.gov.au/news/news/Pages/attribution-of-chinese-cyber-enabled-commercial-intellectual-property-theft.

49 The 2016, 2017, 2018 editions of the German Federal Ministry of the Interior's Annual report on the protection of the Constitution document a broad range of continuing Chinese intelligence activities against Germany, which the reports frame as threats to economy and national security, see Bundesmit fur Verfassungsschutz, "Annual Reports", (2020): https://www.verfassungsschutz.de/en/public-relations/publications/annual-reports.

the UK,[50] and Canada[51] have all identified intellectual property theft as a cybersecurity issue, though they emphasized its relationship to other kinds of security to various degrees. Likewise, these countries have differed in their willingness to explicitly single out China as the main perpetrator, most likely out of fear of provoking Beijing.

Socialization

The first effort at socializing the norm toward China was through naming and shaming (or stigmatization) by the U.S., both in national reports on IP theft, through public attribution, indictments and the threat of sanctions. Following this mounting pressure, Chinese president Xi Jinping agreed to a U.S. proposal that neither country would steal the other's IP for commercial gain. It remains unclear what the underlying Chinese reasons were, meaning actors may have shared expectations on proper behavior but for vastly different reasons or interests. After all, acceptance of a norm is not limited to its substance. Improving Sino-American relations and halting increased U.S. pressure and stigmatization was considered a practical and social benefit for the status or reputation of China, which was endeared to adopt the norm not necessarily because of the content, but because of the comfort and improved relations they may enjoy through conformity. It may thereby ostensibly adopt the norm whilst avoiding actual commitment to it – a form of lip service that allows them to skirt the determinantal stigmatization of resistance without altering their behavior.

The 2015 agreement constituted the pivotal moment in the socialization process.[52] China subsequently agreed to similar bilateral agreements with Australia,[53] Canada,[54] Germany,[55]

---

50 The United Kingdom's 2016 National Cyber Security Strategy links IP theft to economic and national security, but does not mention China explicitly, see Government of the United Kingdom, "National Cyber Security Strategy 2016-2021", (2016), p. 39-40: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf,.

51 Canada mentioned IP theft as a threat to cybersecurity in its national strategy but has been comparatively less vocal about the issue and has been reluctant to blame China specifically. See Stephens, Hugh. "Negotiating a Canada-China Trade Agreement – What about IP?", Macdonald-Laurier Institute (30 October, 2017): https://www.macdonaldlaurier.ca/negotiating-canada-china-trade-agreement-ip-hugh-stephens-inside-policy/; Government of Canada, "National Cyber Security Strategy", (2018): https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

52 United States Office of the Press Secretary, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", The White House, (25 September, 2015): https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

53 The bilateral agreement between China and Australia came into power in June 2017: Department of Foreign Affairs and Trade of Australia, "High-Level Security Dialogue With China: Joint Statement", (24 April, 2017): https://www.dfat.gov.au/news/media/Pages/high-level-security-dialogue-with-china-joint-statement.

54 CBC, "Canada and China Sign No-Hacking Agreement to Protect Trade Secrets", (26 June, 2017): https://www.cbc.ca/news/politics/canada-china-no-hacking-agreement-1.4178177.

55 Joint declaration by China–Germany Intergovernmental Consultations from June 2016 promised to setup "bilateral cyber security consultation mechanism" while they also agreed that they will avoid conducting or supporting "the infringement of intellectual property, trade or business secrets through the use of cyberspace in order to attain competitive advantage for their businesses or commercial sector". Consultations then continued throughout 2018 without producing tangible results because the Germans wanted to discuss IP theft while the Chinese preferred to focus on cyberterrorism. See Segal, Adam; Hoffman, Samantha; Hanson, Fergus; Uren, Tom, "Hacking for Ca$h", ASPI, (2018), https://www.aspi.org.au/report/hacking-cash.

and the U.K.[56] In November 2015, Brazil, Russia, and other members of the G20 accepted the same norm.[57] Since the threat of IP theft was also socialized within these states – albeit to a much lesser extent than in the U.S. – there was an opportunity to agree on a similar norm with China by bandwagoning on the U.S. tools of influence as China was already socialized towards accepting the norm. The socialization mechanism accelerated when the G20 was used as the organization platform to institutionalize the norm.[58] This in turn led to an ongoing dynamic of imitation and bandwagoning as norm leaders attempt to socialize other actors to become norm followers. For some actors, it may have been in their interest to agree to this norm, while for others maintaining good relations with their respective partners is both a practical and social imperative for maintaining their own status, interest and values, and thus may have adopted the norm not necessarily because of the content but as a form of social camouflage.

Persuasion

Persuading actors with a very different value and interest system is extremely difficult unless the norm is incompletely theorized. The U.S. combined positive, though intangible, inducements with particular framing narratives to persuade China to accept the norm. *Positive inducements* included promises of improvements to the overall relationship between the two countries, which disappeared soon after bilateral relations deteriorated after the Trump administration took office and a tariff and trade war unfolded. By *framing* the norm within the context of economic benefits (rather than political-military espionage), by *linking* theft of intellectual property to threats to innovation, economic development, and national security, and by identifying China as the main perpetrator, the U.S. was not only able to stigmatize China, but also able to persuade its Western partners of the value of this norm.

Coercion

The U.S. used a combination of coercive tools that together created leverage towards the Chinese agreement of a new norm against IP theft for economic purposes. The coercion was largely conducted through naming and shaming, indictments, and the threat of sanctions. Although these tools were first and foremost intended to punish China's bad behavior, they contributed to the subsequent acceptance of the norm by China through signaling that punishment and stigmatization would continue as long as China would continue with IP theft. Other countries did not have to take similar coercive measures as China already adopted the norm with the United States. Australia, for example, remains reluctant to formally attribute and publicly name and

56 Adam Segal, ,"The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age", Public Affairs (23 February, 2016).
57 G20, "G20 Leader's Communiqué Antalya Summit", (16 November, 2015): https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf.
58 *Ibid.*

shame adversary states engaging in cyber theft for commercial because of the technical uncertainties related to attribution and because of fears of damaging important diplomatic, economic and intelligence relationships.[59]

In sum, this case study has shown that although the norm in question has a relatively short lifespan so far, the wide use of tools of influence led to the Chinese adoption of the norm. At best, the norm was an incompletely theorized norm, meaning the parties agreed but for different reasons. At worst it can be considered an insincere commitment - a form of lip service that allowed China to skirt the detrimental stigmatization of resistance and implement changes to its tactics, techniques and procedures that it already planned to make by reorganizing its intelligence operations away from the PLA and toward the SSF, without the intention of actually altering its own behavior. This would explain the resurgence of Chinese IP theft, which can also be explained by the increased U.S.-China political and trade tensions that took away the incentives for Beijing to continue adhering to the norm.

While China may initially appear to adhere to the norm not because of its content but as part of tactical bargains that serve its 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. The norm confirmation established by incentives may set in motion organizational and bureaucratic processes that facilitate the internalization of the normative habits by codifying norm-compliance expectations in strategies, rules, procedures, doctrines, rules of engagement, training or other means. In their observations of this case study, some experts have stated that Chinese policymakers believe their shift in tactics, techniques and procedures towards the MSS deploys a higher level of tradecraft that is now equivalent to that of the U.S. National Security Agency. If this is the case, Beijing changed its behavior as a result of the norm and outside pressure, but instead of accepting the distinction that Washington promoted between 'acceptable' and 'unacceptable' espionage, they saw it in terms of compartmentalizing its relatively noisy espionage activity to a smaller number and higher level of hacking in line with what it believes the NSA conducts. The Chinese changes in organizational and bureaucratic processes show a change of behavior but not the internalization of the norm the U.S. hoped for when it proposed the 2015 agreement.[60] Finally, China may become *entrapped* by albeit insincere prior rhetorical commitments in ways that push towards norm conformity and sometimes acceptance. The alternative is the danger of appearing hypocritical, which would come with reputational and credibility costs.

---

59 Segal, Adam; Hoffman, Samantha; Hanson, Fergus ; Uren, Tom, "Hacking for Ca$h", ASPI (2018) : https://www.aspi.org.au/report/hacking-cash.

60 Mulvenon, James, "Beyond Espionage: IP Theft, Talent Programs, and Cyber Conflict with China", Fairbank Center for Chinese Studies, (22 April, 2020): https://fairbank.fas.harvard.edu/events/critical-issues-confronting-china-series-10/; https://www.aspi.org.au/report/hacking-cash.

3.3.2 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. If we follow the logic that the return to industrial hacking might be a reaction to the increased political and trade tensions between China and the U.S., we can identify three potential negative externalities tied to unilateral U.S. sanctions.

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. Case study 1 has shown how Russia has weaponized this argument by claiming that the U.S. indictments are simply political actions.[61] 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 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.[62] 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.[63]

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

62 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.

63 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.

The U.S.' sweeping sanctions as part of a bigger trade and tariff war may lead Chinese policymakers to now believe they have little to gain from honoring the agreement. Rather than focusing on targeted sanctions on Chinese companies and organizations caught stealing U.S. intellectual property, U.S. sanctions of Chinese entities have become part of a broader bilateral trade and tariff war. In this conflict, the U.S. has been seeking to impose restrictions on Chinese investment in high-technology sectors, blocking Chinese telecommunication companies from doing business in the U.S., and levying tariffs against Chinese exporters. As a result, Chinese policymakers may now believe they have little to gain from continuing to honor the initial MOU agreement.

The same sweeping sanctions against China, in combination with the tariffs the U.S. levies on its partners, isolates the norm violation and the threat of IP theft as a bilateral US-China issue. Instead, the U.S. should mobilize large-scale, coordinated attribution and subsequent sanctions *with* its partners – other victims that have struck similar norms with China such as Canada, Australia, the U.K. and Germany – in the same coordinated fashion as the countermeasures adopted against Russian hybrid aggression described in the first case study. This need for rethinking the unilateral U.S. approach is described by Adam Segal as follows: "while the Trump administration has so far shown little inclination to work with allies on its China policy, and is levying tariffs on some of these potential partners, a broad coalition would frame industrial cyber espionage as not just a point of contention in the US-China relationship but also as a point of Chinese intransigence in the face of an increasingly accepted international norm."[64]

3.4 Key Takeaways

The U.S. primarily used coercion and socialization, and to a lesser extent persuasion, to convince China to adopt the norm. The U.S. sought to *persuade* China by promising better bilateral ties and its partners by linking the costs of IP theft to its economy and national security whilst framing it in such a way that it would limit conventional political-military espionage operations, *coerce* China to adopt the norm through indictments and the threat of sanctions, and *socialize* the norm with China through stigmatization by using the G20 as a platform. The internalization of the norm by China was contingent upon better US-China relations moving forward. As soon as that positive inducement disappeared, Chinese incentives for internalization diminished.

While the norm and the countermeasures showed promising initial results of Chinese internalization, Chinese behavior now appears to signal an insincere commitment. The so-called return to flouting the established norm may be viewed as the result of souring US-China relations after the departure of the Obama administration and

64 Segal, Adam; Laskai, Lorand, "A New Old Threat", Council on Foreign Relations (6 December, 2018): https://www.cfr.org/report/threat-chinese-espionage.

ramping up of the US-China trade war under President Trump. However, it may similarly be viewed as the unilateral actions of China acting in bad faith – agreeing to curb its economic espionage as a pretext to reconstitute its PLA operations for more effective engagement in the future. While China may initially have appeared to adhere to the norm, not because of its 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. Furthermore, the norm provides an important yardstick as China becomes *entrapped* by the reciprocal consequences of insincere prior rhetorical commitments in ways that push towards norm conformity and potential acceptance. The alternative is the danger of appearing hypocritical, which would come with reputational and credibility costs.

Beijing may have changed its behavior as a result of the norm and outside pressure, but not in the way that Washington promoted the difference between 'accepted' and 'unacceptable' espionage. Alternatively, China rationalized its actions as bringing previously noisy espionage activity under a more concise and manageable number and a higher level of hacking in line with what it believes the NSA conducts. The Chinese changes in organizational and bureaucratic processes show a change of behavior, but no internalization of the norm the U.S. hoped for when it proposed the 2015 agreement.

In its coercive enforcement of the norm, the U.S. should respond targeted and multilaterally, rather than unilaterally. Instead of sanctions targeting specific norm violators, U.S. sanctions of Chinese entities have instead been part of a broader bilateral trade and tariff war. Chinese policymakers might now believe they have little to gain from continuing to honor the norm as bilateral relations worsen regardless. Furthermore, the sweeping sanctions against China, in combination with the tariffs the U.S. levies on its partners, isolates the norm violation and the threat of IP theft as a bilateral U.S.-China issue. Instead, the U.S. should mobilize large-scale, coordinated attribution and subsequent sanctions *with* its partners – other victims that have struck similar norms with China, such as Canada, Australia, the U.K., or Germany – in the same coordinated fashion as the countermeasures adopted against Russian hybrid aggression described in the first case study.

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