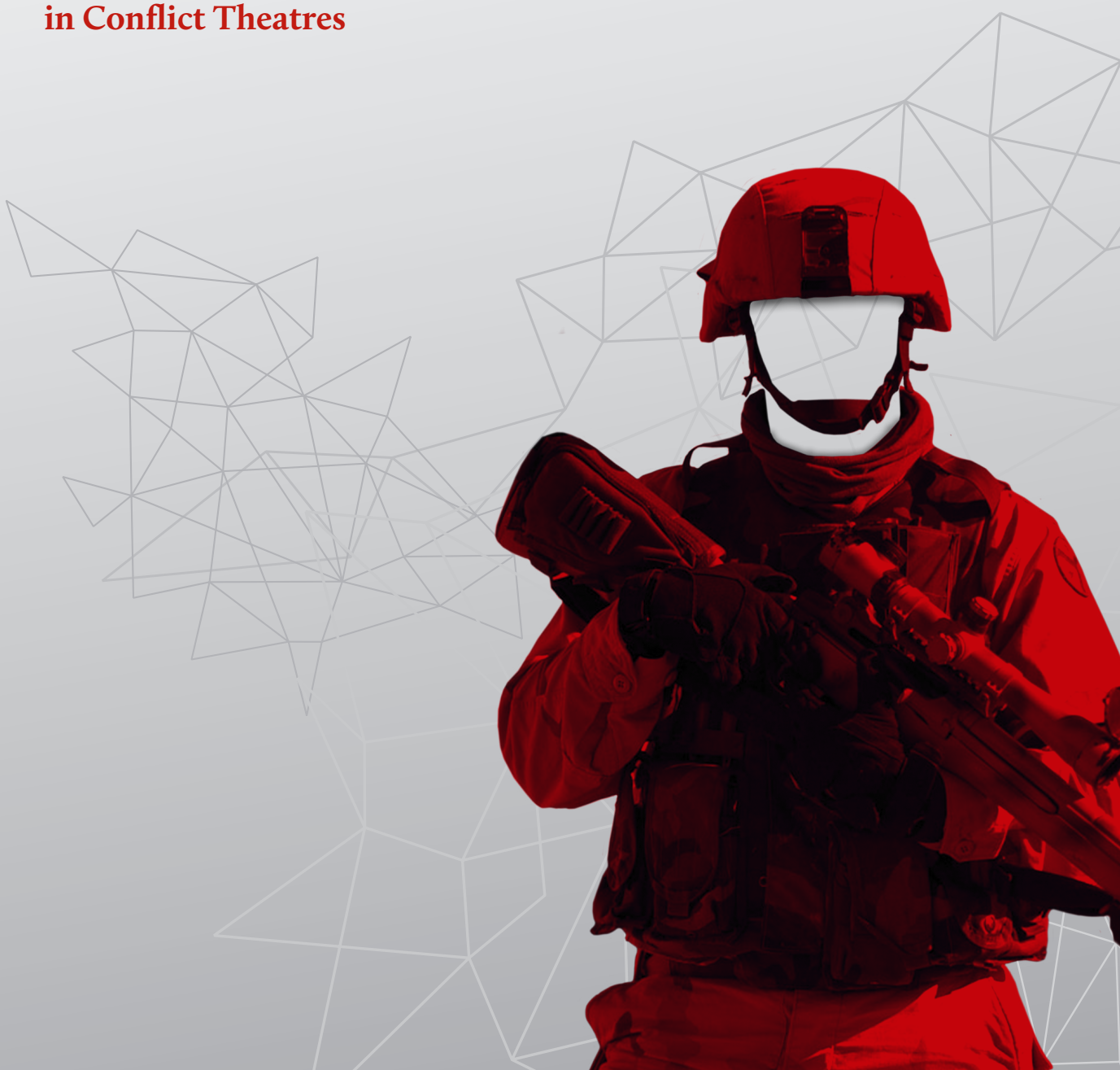
The Hague Centre for Strategic Studies

HCSS PAPER SERIES – CASE STUDY 3

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 3: Countering ISIS Propaganda in Conflict Theatres



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 3

From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 3: Countering ISIS Propaganda in Conflict Theatres

Table of contents

About the Paper Series

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

Paper Series | From Blurred Lines to Red Lines

How Countermeasures and Norms Shape Hybrid Conflict

Case Study 1
Protecting Electoral Infrastructure from Russian cyberoperations

Case Study 2
Responding to Russian disinformation in peacetime

Case Study 3
Countering ISIS propaganda in conflict theatres

Case Study 4
Responding to Chinese economic espionage

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

Read the full report here.

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

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

3

Countering ISIS Propaganda in Conflict Theatres

From 2014, ISIS embarked on a social media campaign to recruit new members. Professional quality print publications and promotional videos were distributed through messaging applications and social media sites.

Countermeasures

Strategic Communication (STRATCOM): The U.S. employed counter narratives to contest ISIS' presence within the social media sphere.

Second-order normative effects

The U.S.' STRATCOM embodied a respect for truthfulness not reciprocated by adversaries (i.e. Russia).

PSYOPS: The U.S used leaflets and broadcasted audio to weaken the support base of ISIS.

The incomplete account of the scope of anti-ISIS PSYOPS makes it difficult to evaluate their normative significance.

Offensive Cyber Operations: USCYBERCOM launched offensive cyber operation 'Glowing Symphony'. It gained access to ISIS accounts, deleted content, crashed servers, and locked ISIS members out of their accounts.

Given the successful outcome of these operation compared to the STRATCOM campaign, U.S. officials have been migrating such wartime campaigns to use against peacetime state adversaries, such as Russia.

Norm proposal

Norm of truthfulness as a benchmark for information operations

This normative yardstick, derived from the IHL principle of proportionality and distinction, stipulates that the broader the target audience and the medium used in influence operations, the more an adherence to truthfulness is required. Inversely, targeted covert influencing operations (e.g. PSYOPS and MILDEC) may leverage a higher degree of falsehoods.

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 American and British countermeasures in cyberspace in response to ISIS propaganda. More specifically, this paper takes a closer look at the underlying mandate of these countermeasures, their second-order normative effects, and whether they reaffirmed existing norms or established new norms.

Despite norms traditionally being instruments that govern peacetime operations, our normative analysis of American wartime countermeasures against ISIS reaffirmed the principles of International Humanitarian Law (IHL) as being fully applicable to cyber and influence operations. Against this backdrop, we explored the possibility of establishing a normative yardstick for truth in Strategic Communication (STRATCOM), information, psychological and other influence operations. This norm derives from the IHL principle of proportionality and distinction in which the broader the target audience and the mediums used (e.g. radio or television), the more truth is prevalent. Inversely, targeted covert influencing operations (e.g. PSYOPS and MILDEC) may leverage a higher degree of falsehoods. The Western normative benchmark of truthfulness has not explicitly emerged, in part because of the clandestine nature of information operation and because the course of action is not yet strong enough to be labeled as habitual. Instead, the principle comparative value of this inception norm

resides in the way that American countermeasures in the information environment were conducted during wartime against a non-state entity compared with the previous case examination of a peacetime response to Russian disinformation. On the one hand, the Western approach is contrasted with the ISIS and Russian Information Warfare doctrines, which make no distinction between peacetime and wartime countermeasures and readily engage in disinformation and propagation across broad public media channels without regard for their collateral damage, as evidenced in case study 2. On the other hand, the need for such a norm may become more evident as these wartime measures are migrated to a peacetime environment.

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: Countering ISIS Propaganda in Conflict Theatres

The norm lifecycle provides the theoretical basis through which we can now analyze norm development in a case study to better understand the real-life strategies, tools of influence, dilemmas, and trade-offs that empower state-led norm processes. The dynamics between countermeasures and norms are analyzed as part of the strategies adopted by the U.S. and European countries toward ISIS propaganda, and how they can potentially establish a normative yardstick for truth in Strategic Communication (STRATCOM), information, psychological and other influence operations

Despite norms traditionally being peacetime instruments, our normative analysis of U.S. wartime countermeasures is centered around the principles of International Humanitarian Law (IHL). We then 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. 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, while 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 ISIS propaganda efforts, 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 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, information, and military countermeasures in response to ISIS propaganda.

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

Building upon its military successes in early 2014, ISIS launched a massive propaganda effort to target foreign audiences. It was intended to secure control over its conquered territory by legitimizing the theological credentials of its proto-caliphate; to inspire foreign emigration to its territory, and to recruit professionals for its movement.[12] For the purposes of recruitment, ISIS built its narratives around the themes of urgency, the agency of individual Muslims, the authenticity of its declared caliphate, and propagating the inevitability of its victory via scriptural allusions to the prophesized apocalypse in their main online outlet *Dabiq*.[13] The recruitment campaign centered on nine attributes for appealing to potential fighters and non-combatant professionals: status-seeking, identity seeking, revenge, redemption, thrill, ideology, justice, and death.[14]

11 Jong, de Sijbren; Sweijs, Tim; Kertysova, Katarina; Bos, Roel, "Inside the Kremlin House of Mirrors", The Hague Centre for Strategic Studies, (17 December, 2017), p. 9: https://hcss.nl/sites/default/files/files/reports/Inside%20the%20Kremlin%20House%20of%20Mirrors.pdf.
12 Harleen Gambhir, "The Virtual Caliphate: ISIS'S Information Warfare", Washington: Institute for the Study of War, (8 December 2016) pp. 9–20: http://www.understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf.
13 Fernandez, Alberto, "Here to Stay and Growing: Combating ISIS Propaganda Networks", U.S.-Islamic World Forum Papers, Brookings, (October 2015), pp.11–12.; Revkin, Mara; McCants, William: "Experts Weigh in (part 5): How Does ISIS Approach Islamic Scripture?", Brookings Institute (2015): https://www.brookings.edu/blog/markaz/2015/05/13/experts-weigh-in-part-5-how-does-isis-approach-islamic-scripture/.
14 Tucker, Patrick, "Why Join ISIS? How Fighters Respond When You Ask Them". The Atlantic, (9 December, 2015).

The group utilized multidisciplinary personnel of editors, videographers and veterans of the Salafi-Jihadi movement and a smaller cadre of former high-level Ba'athist members in its propaganda campaign.[15] Its technical capabilities combined a centralized managerial hierarchy with a decentralized server network to propagate its tailored material through online social media platforms, encrypted apps like WhatsApp[16] and Telegram[17], and deep web publications such as its flagship publication *Dabiq*.[18] The operational goal was to reach general audiences on public media platforms and draw them down the levels of progression towards the deep web and communication channels.[19] The milestone of increased dissemination of propaganda occurred in the spring of 2014 with a series of short reports, tweets and videos. The most sophisticated of these efforts was the landmark video series called "Clanging of the Swords, Part Four".[20] Its footage was more than one hour long and it included violent depictions ISIS' recent military triumphs.[21] More videos, though shorter in length, followed in the aftermath of the fall of Mosul on June 10, 2014. All these videos included commentaries or subtitles in German or English to reach Western audiences, and some deliberately omitted gruesome details to allow for greater dissemination by tailoring them to Western media reporting, which developed a reliance on such content due to the absence of direct reporting of its own due to the danger posed to journalists on the ground.[22]

3.2 Countermeasures

We can distinguish between three kinds of countermeasures employed against ISIS' propaganda: (1) strategic communication as part of a broad communication campaign of the U.S. State Department which was later supplemented by U.K. and EU efforts, (2) psychological and information operations as, and (3) cyber operations.

Strategic Communication (STRATCOM) was initially the focal point of U.S. countermeasures; this approach was predicated on "focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve

15 Whiteside, Craig, "A Pedigree of Terror: The Myth of the Ba'athist Influence in the Islamic State Movement", Perspectives on Terror 11, no. 3, (2017): http://www.terrorismanalysts.com/pt/index.php/pot/article/view/605/html.
16 CBS, "Facebook Says It's Using Artificial Intelligence to Help it Combat Terrorist's Use of Its Platform", (15 June, 2017): https://www.cbsnews.com/news/facebook-using-a-i-artificial-intelligence-against-terrorism/.
17 Winter, Charlie; Amarasingam, Amarnath, "The Decimation of ISIS on Telegram is Big, But it has Consequences", WIRED, (2 December, 2019): https://www.wired.co.uk/article/isis-telegram-security.
18 Gambhir, Harleen, "The Virtual Caliphate: ISIS'S Information Warfare", Institute for the Study of War, (2016), p.20.
19 Kernan, Erik, "The Islamic State as a Unique Social Movement: Exploiting Social Media in an Era of Religious Revival", University of Vermont, (2017): https://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1227&context=hcoltheses.
20 Aalst, Max van: "Ultra-Conservatism and Manipulation: Understanding Islamic State's Propaganda Machine", Leiden University, (2016): https://openaccess.leidenuniv.nl/bitstream/handle/1887/53658/2016_Aalst_CSM.pdf.
21 Fernandez, Alberto, "Here to Stay and Growing: Combating ISIS Propaganda Networks", U.S.-Islamic World Forum Papers, Brookings, (October 2015), pp.8–9.
22 Williams, Lauren: "Islamic State Propaganda and the Mainstream Media", Lowy Institute for International Policy, (1 February, 2016): https://www.jstor.org/stable/resrep10163?seq=3#metadata_info_tab_contents; Fernandez, Alberto, "Here to Stay and Growing: Combating ISIS Propaganda Networks", U.S.-Islamic World Forum Papers, Brookings, (October 2015), p. 9–10.

conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power."[23] From late 2013, the U.S. State Department launched its "Think Again, Turn Away" campaign to counter online Islamist propaganda.[24] Its purpose was to hinder the effects of ISIS propaganda, specifically to dissuade young people from joining the movement and amplify accounts from ISIS defectors. This campaign was pursued across multiple platforms using multilingual counter-material including YouTube, Facebook and Twitter.[25] The most highly viewed video of the campaign appeared on July 23, 2014, titled "Welcome to the Islamic State Land". It depicted the brutality of ISIS by including original footage of the movement's attacks and executions.[26] Supplementary engagement via Twitter sought to deprive ISIS of a monopoly on the media narrative through regular exchanges, pointing out the flaws in the movement's arguments and ideology.[27] The effectiveness of these measures remains inconclusive, but several commentators have criticized the efforts for being ineffective or inadvertently amplifying and consequently legitimizing ISIS' media campaign in the eyes of some receptive audiences, consequently decreasing U.S. credibility.[28]

Mandate STRATCOM: The U.S. Department of State is the leading organization when it comes to strategic communication. The initial campaign was conducted by its Center for Strategic Counterterrorism Communications (CSCC), of which the Digital Outreach Team is most relevant as it aimed to "contest the space, redirect the conversation, and confound the adversary."[29] In early 2016, the center was absorbed by a new Global Strategic Engagement Center (GSEC) that also includes personnel from the Department of Defense, the National Counterterrorism Center, the intelligence community and other U.S. government entities involved with strategic communication.[30]

One of the most well-known domestic anti-propaganda laws within the U.S. is the Smith-Mundt act that prohibits the U.S. government's propaganda efforts from reaching American citizens.[31] While the act does not prohibit the use of propaganda against foreign entities, it does invoke a more cautious approach to its broadcasting efforts, and it significantly limits them as they may not reach any U.S. citizens. While this act has been subject to many amendments, including one in July 2013[32] that loosened it to U.S. consumption, it's not yet clear to what extent the amendment changed the mode of operation and the scope of the STRATCOM efforts.

23 U.S. Department of Defense, "Strategic Communication Joint Integrating Concept", (7 October 2009), B-10: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jic_strategiccommunications.pdf?ver=2017-12-28-162005-353.

24 Miller, Greg; Higham, Scott, "In a Propaganda War Against ISIS, the U.S. Tried to Play by the Enemy's Rules", Washington Post, (8 May, 2015): https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-to-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html.

25 Fernandez, Alberto, "Here to Stay and Growing: Combating ISIS Propaganda Networks", U.S.-Islamic World Forum Papers, Brookings, (October 2015), p.14–16.

26 *Ibid*. p.15.

27 Katz, Rita, "The State Department's Twitter War With ISIS Is Embarrassing", TIME, (16 September 2014): https://time.com/3387065/isis-twitter-war-state-department/.

28 Katz, Rita; Bilazarian, Talene, "Countering Violent Extremist Narratives Online: Lessons From Offline Countering Violent Extremism", Policy and Internet 12, no. 1 (March 2020), pp.46–65: https://doi.org/10.1002/poi3.204.;

29 The Obama administration established the Center and delineated its competencies by Executive Order 13584 in 2011. United States Office of the Press Secretary, "Executive Order 13584 --Developing an Integrated Strategic Counterterrorism Communications Initiative", The White House, (9 September 2011).; Fernandez, Alberto, "The State Department's Center for Strategic Counterterrorism Communications: Mission, Operations, and Impact: Hearing before the Subcommittee On Terrorism, Nonproliferation, and Trade of the Committee On Foreign Affairs", House of Representatives, (2 August 2012): https://www.govinfo.gov/content/pkg/CHRG-112hhrg75389/html/CHRG-112hhrg75389.htm.

30 The Trump administration has reportedly gutted the GSEC, which previously countered terrorist propaganda and is now tasked with disinformation at a global scale. At the same time Congress pushed for "the State Department needs to be a full partner in developing a strong and credible counternarrative, which requires more nuance and range than traditional counterpropaganda."; Slaughter, Anne-Marie; Castleberry, Asha, "Islamic State 2.0 and the Information War", Australian Strategic Policy Institute, (2 October, 2019): https://www.aspistrategist.org.au/islamic-state-2-0-and-the-information-war/; Office of the Spokesperson, 'A New Center for Global Engagement', U.S. Department of State, (8 January 2016): https://2009-2017.state.gov/r/pa/prs/ps/2016/01/251066.htm.

31 Throrberry, Mac, "H.R.5736 – Smith Mundt Modernization Act of 2012", House Committee on Foreign Affairs, (10 May, 2012): https://www.congress.gov/bill/112th-congress/house-bill/5736.

32 Klimburg, Alexander, "The Darkening Web: The War for Cyberspace", Penguin Press, (11 July, 2017).

Mandate PSYOPS and Information Operations: With respect to U.S. psychological operations and specifically the information operations of the second phase of Operation Glowing Symphony, the governing doctrinal mandate is Joint Publication 3-13 on *information operations*, and is further specified in JP3-13.2 *psychological operations*. JP 3-13 is the keystone document in understanding the U.S. military approach to information operations, which is described "as having five specific components or dimensions: computer network operations (CNO), psychological operations (PSYOPS), signals (maintaining communication), military deception (MILDEC), and intelligence/counterintelligence."[37] Indeed, the definition of information operations puts an equal emphasis on the cyber component of CNO and the psychological warfare components of PSYOPS and MILDEC. This degree of overlap has produced a level of confusion but also lateral freedom in the conduct of U.S. offensive actions. The document moves information attacks, such as misdirection, propaganda and other psychological operations, to a lower level of conflict, a localized military campaign rather than a national campaign. Information operations are described as a tool used by military brigades and divisions at the tactical or operational level in a theater of war, but not as a strategic weapon that is directed at the political leadership of another nation. The purpose of psychological operations is to "convey messages to selected foreign groups to promote particular themes that result in desired foreign attitudes and behaviors" and "shape the security environment to promote bilateral cooperation, ease tension and deter aggression".[38]

Mandate: Red, Blue and Gray Cyberspace: According to JP 3-12, the view of cyberspace based on location and ownership is categorized into three criteria: red, blue and gray cyberspace. The term "red cyberspace" refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact on the operation of the system.[39] Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. The term "blue cyberspace" denotes areas in cyberspace protected by the U.S., its mission partners, and other areas the Department of Defense or other U.S. cyber forces may be ordered to protect.[40] All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.[41]

Psychological Operations (PSYOPS) constituted the latter part of U.S. military intervention via the *Military Information Support Task Force – Central* (MISTF-C) at the operational and tactical level to weaken the support base of ISIS by highlighting the corrupt nature of the organization's leadership and the inherent faults of its ideology. There is very little public knowledge about the nature of these operations given their classified nature. Media reporting or released documents from FOIA requests show that U.S. PSYOPS mainly focuses on broadcast audio messages and the dropping of leaflets.[33]

Finally, the U.S. also used offensive cyber operations through the launch of Operation Glowing Symphony by USCYBERCOM in November 2016. It was tasked with countering ISIS online media operations and propaganda and considered to be the largest and most complex publicly known offensive cyberspace operation USCYBERCOM has conducted to date.[34] The operation was led by Joint Task Force Ares (JTF-ARES), which identified a core network of ten accounts used by ISIS as the distribution node for their online propaganda campaign.[35] The operational tactics employed began with coordinated phishing emails, followed by malware insertions into ISIS servers. The task force spent months proving that they could successfully attack ISIS content hosted on civilian severs without harming other content, before being granted authority to launch a more pronounced attack.[36] The task force deleted ISIS files, IPs, and accounts.

33 Trevithick, Joseph, "U.S. Psyops Blasted ISIS With Recordings of Crying, Troops Retreating, and Other Confusing Audio", The Drive (14 December 2018): https://www.thedrive.com/the-war-zone/25504/u-s-psyops-blasted-isis-with-recordings-of-crying-troops-retreating-and-other-confusing-audio.

34 Martelle, Michael, "USCYBERCOM After Action Assessments of Operation Glowing Symphony", NSA Archives: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

35 Temple, Raston, "How the U.S. Hacked ISIS", NPR (26 September 2019): https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis; Pomerleau, Mark, "What Cyber Command's ISIS Operations Mean for the Future of Information Warfare", CYISRNET, (19 June, 2020): https://www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/.

36 *Ibid*.

37 United States Army, "Joint Publication 3-13 Information Operations", (27 November, 2012): https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf; Klimburg, Alexander, 'Darkening Web', Penguin Press, (11 July, 2017).

38 United States Joint Forces Development, "Joint Publication 3-13.2: Psychological Operations", (07 January 2010): https://docplayer.net/130546119-Joint-publication-psychological-operations.html.

39 Joint Forces Development: "Joint Publication 3-12: Cyber Operations", (8 June, 2018), p. 24.

40 *Ibid.*

41 *Ibid.*

Thereafter, the second phase of Operation Glowing Symphony consisted broadly of five operational goals, according to subsequent media reporting:[42]

- Maintain pressure on ISIS media operations
- Make it difficult for ISIS to operate online more generally
- Use cyber to help conventional coalition forces on the ground fighting ISIS
- Hobble ISIS' ability to raise funding
- Cooperate with other U.S. and allied agencies

The second phase of Operation Glowing Symphony focused on information operations that were disguised as mundane inconveniences: slow internet speeds, dropped connections, embedded glitches and lost passwords.[43] An operational tactic was to frustrate ISIS operators and sow discord by degrading their lines of communication and concealing sabotage as the failings of an incompetent IT department. Within six months of the operation's launch, ISIS' media operation was severely degraded – its network of servers were down and they were unable to reconstitute them. The online publication *Dabiq* – a cornerstone of ISIS' recruitment strategy – ultimately folded in part due to the operational difficulties imposed by Operation Glowing Symphony, in tandem with the deaths of a number of irreplaceable editorial staff through coalition, the Syrian army, and rebel incursions into ISIS territory.[44]

Mandate Cyber Operations: Within the U.S. a distinction is made between Title 50 (offensive operations) and Title 10 authorities (covert intelligence operations).[45] The latter falls under US, not international, law. The described offensive operation is a Title 50 authority that, however, is covered by international law. The domestic legal basis for the U.S. cyber operations is under the National Defense Authorization Act and revised 10 U.S.C. § 394, which expanded the authority of the Defense Department to operate in the cyber domain.[46] At the same time, President Trump replaced Obama's Presidential Policy Directive 20 with the National Security Presidential Memorandum 13. This is a confidential document that was not made public. It, therefore, remains unclear what the new authorization process for offensive cyber operations looks like exactly, but it appears that decisions can now be made at a lower level by the head of CYBERCOM without interdepartmental approval from the State Department.[47]

Additionally, the Joint Publication 3-12 on Cyberspace Operations sets forth the joint doctrine to "govern the activities and performance of the Armed Forces of the United States in joint operations, and considerations for military interaction with other governmental and non-governmental agencies."[48] As a guiding document, it outlines the relationships between the Joint Staff (JS), USCYBERCOM, the Service Cyberspace Component (SCC), the Combatants Commands (CCMDs), and combat support agencies; this framework provides a framework for how the U.S. employs its cyberspace capabilities.[49]

42 Temple, Raston, "How the U.S. Hacked ISIS", NPR (26 September 2019): https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

43 Martelle, Michael: "USCYBERCOM After Action Assessments of Operation Glowing Symphony", NSA Archive (21 January, 2020): https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

44 Goldman, Adam; Schmitt, Eric: "One By One, ISIS Social Media Experts are Killed as Result of F.B.I. Program", New York Times, (24 November 2016): https://www.nytimes.com/2016/11/24/world/middleeast/isis-recruiters-social-media.html.

45 For more information about the Title10-Title 50 debate see Wall, Andru, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities and Covert Action", Harvard College (2011): https://www.soc.mil/528th/PDFs/Title10Title50.pdf.

46 The National Defense Authorization Act specifically notes that "the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber-attacks or other malicious cyber activities of foreign powers that target the United States". It emphasizes cyber operations as being a component of traditional military activity, for the purposes of attaining legal status as covert action – a traditionally vague area of international law. United States Code: "10 U.S.C. § 394", Statues, Codes, and Regulations – United States Code: https://casetext.com/statute/united-states-code/title-10-armed-forces/subtitle-a-general-military-law/part-i-organization-and-general-military-powers/chapter-19-cyber-matters/section-394-authorities-concerning-military-cyber-operations; "H.R.5515- John S. McCain National Defense Authorization Act for Fiscal Year 2019", Congress.gov: https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

47 According to some experts, the elimination of PPD-20 translates into a significant blow to the State Department's ability to block offensive cyber operations that might conflict with international law and undermine the discussions on norms for state behavior in cyber space. Soesanto, Stefan, "The Evolution of US Defense Strategy in Cyberspace (1988-2019)", Center for Security Studies, Zurich 2019: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf.

48 United States Joint Forces Development: "Joint Publication 3-12 Cyberspace Operations", (8 June, 2018): https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

49 *Ibid*.

The U.S. example was followed by others, including the U.K., which launched the Counter-Daesh Communications Cell and a Global Coalition Website aimed at countering the ISIS narrative and to reduce the effects of its propaganda.[50] The U.K. government employed five lines of action to defeat ISIS, one of which focused on strategic communication.[51] Through joint efforts with over 30 coalition countries, the U.K. sent daily media packages covering ISIS' atrocities and recommending STRATCOM countermeasures to upskill countries with less communications experience; the Cabinet Office notes "this has resulted in numerous partners using strategic coms much more effectively to counter extremism and radicalization in their own countries."[52] Internally, STRATCOM efforts were conducted in a full-spectrum approach across government, Ministry of Defence, Home Office and others in tackling ISIS' propaganda efforts in a collective meta counternarrative.[53] These initiatives focused on a fact-based refutation of the ISIS narrative, undermining their image as victors by propagating the message that they were losing on the ground, as well as presenting a positive vision for the region.[54] There is no evidence that these initiatives effectively engaged with ISIS on social media, as the U.S. had failed to achieve. Social media platforms regularly deleted ISIS accounts upon being made aware of them by authorities.[55] As a result of these collective measures, ISIS was forced out of the online media mainstream, relying instead on less accessible deep web platforms.

In summary, the U.S. response to ISIS propaganda, which the U.K. later joined through its own initiatives, employed a broad range of information operations measures encompassing strategic communications, targeted influence operations, and offensive cyber-attacks.[56] The fact that the body of international law has yet to catch up with the actions employed by the U.S. has so far granted considerable freedom in the conduct of these operations, as ISIS status as an unrecognized state/non-state hybrid actor does not easily adhere to applications of traditional international law.[57] Acknowledging this, the following section addresses the normative components of U.S.' countermeasures and their second-order implications for other aspects of U.S. policy in responding to hybrid threats.

---

50 UK Government, "UK Action to Combat Daesh", (Online: UK Government), accessed 4 April 2020, https://www.gov.uk/government/topical-events/daesh/about.

51 Chugg, Dan: "Winning the Strategic Communications War with Daes", Cabinet Office, (20 December, 2017): https://quarterly.blog.gov.uk/2017/12/20/winning-the-strategic-communications-war-with-daesh/.

52 *Ibid.*

53 *Ibid.*

54 *Ibid;* For more details, see the website of the Coalition: The Global Coalition Against Daesh. "News & Analysis." (2020): https://theglobalcoalition.org/en/news-analysis/.

55 Ahmad Shehabat and Teodor Mitew, "Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics", Perspectives on Terrorism 12, no. 1 (February 2018) pp.83–84.

56 Aragó, Bernat: "Media Jihad", European Institute of the Mediterranean (2017): https://www.iemed.org/observatori/arees-danalisi/arxius-adjunts/quaderns-de-la-mediterrania/qm24/Media_Jihad_Bernat_Arago_QM24.pdf.

57 Edwards, Holli: "Does International Law Apply to the Islamic State", Geneva Centre for Security Policy (2017): https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/GCSP-SSA1-2017-UNGERER%20and%20EDWARDS%20-Draft7%20Final.pdf.

3.3 The Normative Dimension: What Norms are Promoted?

The principle value of analysis of this case study is the means by which U.S. information operation countermeasures were conducted during wartime against a non-state entity, compared with the previous case examination of a peacetime response to Russian disinformation, and the evolving overlap therein. It should be noted that norms are traditionally instruments that govern peacetime operations, whereas wartime operations are governed by laws and principles of International Humanitarian Law (IHL). In lieu of peacetime norms, this section will, therefore, assess if the countermeasures – both in the information and in cyberspace – reaffirm IHL principles. Because a significant part of the tactical details of these operations remains undisclosed, their application to the IHL principles remains limited to disclosed details of the "Think Again, Turn Away" STARTCOM campaign and of the cyber and information operation conducted as part of Operation Glowing Symphony. Subsequently, it will explore the possibility of establishing a normative yardstick for truth in STRATCOM, information, psychological and other influence operations. This norm derives from the principle of proportionality and distinction in which the broader the target audience and the mediums used (e.g. radio or television), the more truth is prevalent. Conversely, the more targeted the operation, such as targeted covert influencing operations within a military mission, the less prominent the need is for truth as the benchmark. The Western benchmark of truthfulness is contrasted with the ISIS and Russian Information Warfare doctrines which make no distinction between peacetime and wartime countermeasures and readily engages in disinformation and propagation across broad public media channels as evidenced in the previous case study. With this comparison in mind, the following sections outline these dimensions in their distinct categories, and in their wider second-order implications.

3.3.1 Affirmation of Existing Norms?

It should be noted at the outset that our analysis is based on publicly available records which, while expansive given recently released documentation obtained from FOIA requests, may not represent a comprehensive account of U.S. actions or its normative impacts. Nevertheless, it is safe to say that the U.S. affirmed IHL principles of proportionality, necessity and distinction by taking feasible precautions in its strategic communications and by exercising caution in engaging a wartime enemy on civilian platforms (social media) and targeting servers located outside ISIS control.

The initial U.S. and subsequent U.K. countermeasures focused on STRATCOM counternarratives to contest ISIS, primarily on social media platforms. This was conducted in tandem with partnerships with social media companies to remove ISIS content and deny them easy access to the wider public, largely due to the excoriations of European governments at social media companies' previous failings to police online

content.[58] In the U.K., referrals from the Counter Terrorism Internet Referral Unit led social media companies to remove 46,000 pieces of terrorist propaganda and a further 55,000 in 2015.[59] The lack of disinformation in STRATCOM countermeasures reflects the fact-based approach such operations typically take in the West versus the strategy of actors like Russia and China. Both components of U.S. STRATCOM – the Digital Engagement team and Web Operations team – adhered to a three-pronged approach that sought to *emphasize* or *deemphasize* specific points of information, rather than creating falsehoods or disinformation, particularly in amplifying stories by ISIS' defectors. This approach thus reaffirmed the applicability of customary International Humanitarian Law (IHL) principles relating to disinformation embodied within the Tallinn Manual, which stipulate that misinformation may be used to mislead adversaries but must distinguish between civilians and combatants[60] and cannot harm the former to in pursuit of the latter.[61] The law itself is dubious in applying to cyberspace, notably in suggesting that "media used for military purposes may be lawfully attacked"[62] but not detailing *how* this distinction is to be made in regard to the complex role of social media platforms as potential dual-use vectors of information operations. Despite this legal ambiguity, the U.S. STRATCOM campaign showed careful regard for its actions in social media, adhering to a fact-based campaign of strategic communications and avoiding the type of malign information operations typical of actors like Russia that operate widely across communication platforms. Specifically, the U.S. regard for a fact-based benchmark in information operations starkly contrasts with the relativist doctrine of Russian campaigns which utilize a so-called 'plurality of truth' to spread falsehoods in broad- scale information warfare.[63]

The U.S. information operations also sought to reaffirm by their actions the principle of proportionality. The precautionary principle of IHL mandates that each belligerent party bears a duty to employ only those methods of warfare whose effects can be contained; any form of information warfare must take "feasible precautions" of

58 Kean, Thoms; Hamilton, Lee; Misztal, Blaise; Hurley, Michael; Danforth, Nicholas; Michek, Jessica. "Digital Counterterrorism: Fighting Jihadists Online" ¸ Bipartisan Policy Center (March, 2018): p. 18.

59 Home Department of the United Kingdom: "CONTEST – The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2015", (July 2016): p. 15.

60 Determining the legal status of an individual under IHL presents difficulties. Overall, ISIS members who directly participate in hostilities in Syria and Iraq may be lawfully targeted by military operations. Edwards, Holli. "Does International Law Apply to the Islamic State?", Geneva Centre for Security Policy, no.1 (2017): https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/GCSP-SSA1-2017-UNGERER%20and%20EDWARDS%20-Draft7%20Final.pdf; Paulussen, Christophe; Cuyckens, Hanne; Fortin, Katharine, "The Prosecution of Foreign Fighters Under International Humanitarian Law: Misconceptions and Opportunities", International Centre for Counter-Terrorism, (13 December 2019): https://icct.nl/publication/the-prosecution-of-foreign-fighters-under-international-humanitarian-law-misconceptions-and-opportunities/.

61 GroJIL: "The Truth Under Siege: Does International Humanitarian Law Respond Adequately to Information Warfare?", Groningen Journal of International Law (2019): https://grojil.org/2019/03/21/the-truth-under-siege-does-international-humanitarian-law-respond-adequately-to-information-warfare/..

62 Schmitt, Michael: "Tallinn Manual on the International Law Applicable to Cyber Warfare", NATO (2013): http://csef.ru/media/articles/3990/3990.pdf.

63 Meister, Stefan: "Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia", Institut für Auslandsbeziehungen (2018): https://www.ssoar.info/ssoar/bitstream/handle/document/59979/ssoar-2018-meister-Understanding_Russian_Communication_Strategy_Case.pdf.

its effects.[64] This extends to prohibiting "incidental loss or damage to civilian life in excess of concrete or direct military advantage".[65] With regard to STRATCOM, the U.S. adheres to a posture of using "factional information of approved narratives" whereas actors like Russia dismiss the collateral damage of their (dis)information operations. Russia's refutation of this concern derives from their official stance that they act in furtherance of available information 'anticipating' a military advantage, as they did before the European Court of Human Rights in response to Georgia's claims concerning (amongst other violations) disinformation by Russia during the South Ossetian War.[66]

Even within its cyber operations, the U.S. showed a level of regard for proportionality and distinction that would not cause collateral damage to the civilian content through which ISIS interspersed their operations. Upon the discovery of ISIS' material hosted on servers alongside unaffiliated civilian content, CENTCOM opted to demonstrate in repeat incidences that it could effectively target the ISIS content without infringing upon the civilian content.[67] This level of proven avoidance to collateral damage was necessitated by the growing "red space" as servers hosting ISIS content were discovered; ultimately this included 35 countries, at least two of which were European allies and one of which – Germany – was especially wary of U.S. cyber interference in the aftermath of the Snowden leaks.[68] In such context, adherence to IHL principles becomes difficult as enemy presence extends beyond the immediate conflict zone into neutral and even allied countries abroad, raising doubts over the scope and applicability of mission mandates. The U.S. solution to this quandary was to reclassify previously viewed civilian gray space and extend operations to engage enemies within all theatres of cyberspace as designated 'red space'.[69] This entails challenging the enemy with targeted-albeit-not-unilateral action anywhere their presence extends to, rather than simply the nodes they control as part of their red space.[70] In U.S. targeting of foreign servers hosting ISIS' content across six countries, USCYBERCOM took due

64 "Principle of Precautions Against the Effects of Attack", ICRC- IHL Database https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule22.

65 Choudhary, Vishakha: "The Truth Under Siege: Does International Humanitarian Law Respond Adequately to Information Warfare?", Groningen Journal of International Law (21 March, 2019): https://grojil.org/2019/03/21/the-truth-under-siege-does-international-humanitarian-law-respond-adequately-to-information-warfare/.

66 Kahn, Jeffrey: "Oral Argument in Georgia v. Russia (II): The Fake News Era Reaches Strasbourg", Lawfare (31 May 2018): https://www.lawfareblog.com/oral-argument-georgia-v-russia-ii-fake-news-era-reaches-strasbourg.

67 Temple-Raston, Dina: "How the U.S. Hacked ISIS", NPR (26 September, 2019): https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

68 Watt, Nicholas; Mason, Rowena: "Angela Merkel Phone-Bugging Claims are Result of Snowden Leaks, MP Claims", Guardian, (24 October 2013): https://www.theguardian.com/world/2013/oct/24/angela-merkel-bugging-snowden-leaks-mp.

69 Net Politics: "U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace", Council on Foreign Relations, (22 April, 2020): https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace; Smeets, Max: "US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection", Intelligence and National Security 35 (3), (15 February, 2020), pp. 444-453: https://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1729316?scroll=top&needAccess=true&journalCode=fint20.

70 Smeets, Max: "Cyber Command's Strategy Risks Friction With Allies", Lawfare (28 May 2019): https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

regard to comply with IHL principles through forewarning and coordination with the host nations to remove the ISIS presence.[71]

3.3.2 A New Norm Emerges?

Based on the available literature, the West uses truth as a yardstick when it conducts different kinds of operations in the information environment. The broader the target audience and of an operation and the medium used (e.g. STATCOM) typically the higher value is placed on truth; inversely, targeted covert influencing operations may leverage a higher degree of falsehoods. This is not the case with other actors, notably Russia, who employ a more generalist approach that does not hold to the same strict distinction between these categories.

As a disclaimer, the normative dimensions of this case do not readily adhere to the norm lifecycle as do the other cases, due to the fact that peacetime norms do not typically apply during wartime, which is regulated by International Humanitarian Law. Unlike the other cases, the novelty of the counter-ISIS case study does not present clear categories of persuasive and coercive tools of influence. Rather, it links previous case studies in informing how U.S. cyber doctrine has developed and what the potential second-order consequences are likely to be in the long term. Compared to the previous case study, wherein the U.S. self-disclosed its actions against a peacetime Russian adversary and by extension imparted a normative shift, much of its wartime actions do not require disclosure and may not affect wider norms. Indeed, the details of Operation Glowing Symphony were only obtained through a freedom of information request in 2018, after which the DoD embraced the success of the operation as an archetype for future actions.[72] This touting of the methods used in Glowing Symphony was not reflected across other government agencies, with noted objections from the CIA, State Department and FBI regarding operating in foreign countries that hosted servers with ISIS data without prior notification.[73]

Nevertheless, an emergent norm that can be derived from STRATCOM's operations was the degree to which truthfulness (fact-based refutations rather than disinformation) acts as a yardstick to larger-scale U.S. operations, i.e. those that do not target individuals. This careful adherence to truthfulness in broad range strategic communication, in this

71 Nakashima, Ellen, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies", Washington Post (9 May 2017): https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

72 Martelle, Michael: "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY", NSA Archive (2020): https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

73 See document 5: USCYBERCOM, "30-Day Assessment of Operation Glowing Symphony", p.17; Martelle, Michael: "USCYBERCOM After Action Assessment of Operation GLOWING SYMPHONY", National Security Archive (21 January, 2020): https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

case, may have stemmed from the U.S. need to reclaim credibility amongst Muslim populations after successive scandals that lost it legitimacy, notably Abu Ghraib and the rhetoric of the Bush administration in referring to the war on terror as a "crusade".[74] In such circumstances, the need to maintain a focus on 'truth campaigns' was prescient, and drove the U.S. to adopt the emergent norm as the benchmark for its STRATCOM countermeasures.[75] In its STRATCOM operations, the U.S. focused on persuading targeted audiences and contesting ISIS' online by refuting its promises to potential recruits and its overall self-proclaimed legitimacy.

This adherence to truthfulness should not be viewed as an absolute, but rather as a relative benchmark to the scope of U.S. information operations. In targeted operations with a specifically defined scope that do not play out across public channels, an option remains there to deploy a degree of falsehood to influence adversary action, as evidenced in U.S. doctrines of military deception (MILDEC) and psychological operations (PSYOPS).[76] Indeed, the purpose of psychological operations to "convey messages to selected foreign groups to promote particular themes that result in desired foreign attitudes and behaviors" holds no special regard for truthfulness in its need to maintain lateral freedom.[77] This need to retain lateral freedom in the conduct of U.S. offensive actions framed the need for truthfulness in this spectrum of approaches. As tactical elements of information attacks, such as misdirection, propaganda and other psychological operations, disinformation may and indeed must remain permittable. But at the other end of the spectrum, these same elements are avoided at the level of STRATCOM, wherein the centrality of truth seems to be a priority, if for no other reason than as a means to maintain credibility amongst a distrustful target audience.

In maintaining this distinction, the U.S. and its allies seek to reaffirm the integrity of truthfulness in information operations that take place within broad range measures that utilize mass media. If considered a norm, this principle of truthfulness is one which is generally internalized in the West but not with others, most prominently not with Russia or China. Non-state actors like ISIS, or indeed state actors like Russia, do not make the distinction between psychological operations and strategic communication and allow all possible measures and tools regardless of their truthfulness. Also, unlike the Western approach which contains psychological operations to the tactical theater, Russia and ISIS also use it at the strategic level outside of the battlefield.

---

74 McFadden, Crystal: "Strategic Communications: The State Department Versus the Islamic State", Naval Postgraduate School (2017): https://www.hsdl.org/?view&did=813341.

75 Favat, Pete; Price, Bryan: "The Truth Campaign and the War of Ideas", Combatting Terrorism Center (2015): https://www.ctc.usma.edu/the-truth-campaign-and-the-war-of-ideas/.

76 Joint Forces Development: "Joint Publication 3-13.4: Military Deception", (26 January, 2012): https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf; Joint Forces Development: "Joint Publication 3-53: Doctrine for Joint Psychological Operations" (5 September, 2003): https://nsarchive2.gwu.edu//NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf.

77 Joint Forces Development: "Joint Publication 3012.2: Military Information Support Operations", (20 December, 2011): https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf.

Currently, the Russian approach sacrifices foreign perceptions of legitimacy for practical expediency and domestic consumption. Those actors who choose this approach risk provoking hostile measures from the West and escalation from the U.S. in particular. This may take many forms, from diplomatic pressure to economic sanctions and military coercion, and possibly an offensive action by USCYBERCOM. At the same time, the approach allows the actors to shape the environment with a higher degree of flexibility, denying the truth and spreading falsehood as they see convenient for their regime security. Thus, though deemed prohibited in the West, the approach is likely to appeal to those who can offset the potential effects of Western hostile measures for the benefit of greater flexibility.

In conclusion, the U.S. continues to promote adherence to truthfulness as a benchmark for its STRATCOM operations, if not its more targeted information operations. The ineffectuality of the STRATCOM operation compared to the Glowing Symphony operation has issued second-order normative implications for how the U.S. approaches future threats and its broader doctrine. The following section deals with these second-order effects in turn, noting the dangerous erosion in distinctions between wartime and peacetime responses that has occurred in U.S. thinking as a result of its operations against ISIS.

3.3.3 Second-Order Normative Effects of the Countermeasures

States may underestimate or even be unaware that countermeasures may establish new norms that conflict with their own long-term interests. As these norms are in their early emergence, they, and the countermeasures which initially formed them, may produce unanticipated long-term consequences. We will take a closer look at how these effects impact the long-term interests of the states that undertook the countermeasures and the normative initiatives of their opponent. In this case study, we focus on one particular externality associated with the respective countermeasures that are not prohibitive but should be taken into consideration as they have an impact on the development of international norms and could run contrary to the interests of the entrepreneur.

As a result of the success of Glowing Symphony compared to ineffectual STRATCOM efforts, the U.S. may prefer targeted information and offensive cyberspace operations with kinetic effects as a first response in a peacetime environment. It thereby migrates wartime measures into peacetime, where they produce higher second-order normative effects, especially when they are taken overtly. Although U.S. countermeasures in the case of its information operations against ISIS generally held to its stated doctrinal principles and normative commitments, the success of the operation has contributed to the potential of long-term emergent second-order normative consequences. Whilst the U.S. initially restricted its engagement with ISIS to contesting its propaganda via STRATCOM, the inconclusive results of these measures coupled with the success of

the subsequent targeted information operations have influenced debates about future engagements. Indeed, the joint cyber and information operations conducted by JTF-Ares have informed U.S. approaches to similar countermeasures in other contexts, potentially outside of the wartime environment they were intended for. U.S. officials, including National Security Agency Director Gen. Paul Nakasone, who headed the Glowing Symphony operation, have stated that the operation "provided a road map for other task forces [...] including the Russian troll farm that has interfered in U.S. elections."[78]

The second-order normative implications of Operation Glowing Symphony and JTF-Ares more generally have contributed to emerging preferences in U.S. doctrinal thinking for imposed coercion and direct control over an adversary freedom of movement as legitimate, a theme which increasingly characterizes U.S. offensive cyber and information operations.[79] As a second order normative consequence, the success of JTF-ARES has triggered debates within U.S. strategic thinking in transposing effective wartime measures to a peacetime environment.[80] This shift is evident in the compromising of Russia's electrical grid in 2019 by USCYBERCOM (the specific taskforce involved, called Small Russian Group is suspected to be the direct successor to JTF-ARES). The operation contained similar denial and punishment measures utilized in Glowing Symphony.[81] As such, if the U.S. opts to prefer the weaponization of information – viewing it as an attack which gives grounds for escalatory countermeasures – in a peacetime environment against state adversaries, it may produce dangerous and unanticipated second order normative effects that justify Russian and Chinese thinking on information as a weapon and eliminate the Western normative basis upon which they can criticize their opponents. The distinction in this sense is that the risk is not equivalent in a military conflict with clear delineation of conflict parties and permissible action; the context of actors using the same or equivalent countermeasures in a peacetime environment is significantly higher risk.

As it contemplates countermeasures to expected Russian campaigns of disinformation in the upcoming 2020 election in reference to the success of its wartime information operations against ISIS, the U.S. may continue to transpose successful countermeasures from one theatre to another. In doing so it would risk introducing a heightened degree

78 Vavra, Shannon. "Top Secret Documents Show Cyber Command's Growing Pains in its Mission Against ISIS", Cyberscoop (21 January 2020): https://www.cyberscoop.com/cyber-command-pentagon-counter-isis-glowing-symphony-foia/.

79 Jones, Seth. "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare", CSIS (1 October, 2018): https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

80 Nakashima, Ellen. "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election", Washington Post (25 December, 2019): https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

81 Nakashima, Ellen. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on day of 2018 midterms.", (27 February, 2019): https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

of escalation and aggression, as covert offensive cyberspace operations are disclosed in the public domain and consequently underlining a lack of communication.[82] This risk is discussed in greater detail in the previous case study where the U.S. effectively took the Russian Internet Research Agency offline.

The operations of JTF-ARES give rise to the norm of cyberspace as an extension of the multi-domain battlefield, and the power of governments to deny and degrade innovative non-state actors proactively across domains. Some have warned of the ambiguity of international law applied to hybrid actors such as ISIS, and the means by which the U.S. formulated their countermeasures, may give rise to a legal vacuum by which a "cyber realpolitik" may take shape as an emerging norm and challenge established frameworks.[83]

In its emphasis on the offensive in cyberspace as a compensating mechanism for poor resilience, the U.S. may be increasingly defining friendly and enemy-controlled space in such broad terms as to escalate unanticipated second-order effects for other actors present within these dual-use platforms such as social media, including non-state actors unaffiliated to the conflict or even allies.

3.4 Key Takeaways

The U.S. STRATCOM countermeasures embody a respect for 'truthfulness' which is not reciprocated by states like Russia. The West maintains its preservation of fact-based truthfulness as the linchpin of strategic communications, particularly when they are employed across broad range public channels. Whilst the novelty of the ISIS case may have influenced this choice more than internal normative shifts in U.S. thinking, the principle remains that truthfulness retains a prominent position in Western information operations, at least within broad-ranged STRATCOM measures that are likely to engage with a wide civilian target audience or even non-affiliated audiences. Rather than propagating disinformation, the focus remains on emphasizing and deemphasizing aspects of an adversary to sway target audiences and contest their influence, especially on social media platforms. However, the U.S. has preserved its freedom of lateral movement through a willingness to employ falsehoods in targeted covert influencing operations, wherein the goal of influencing target groups or figures typically takes place in a smaller scope than broader STRATCOM operations and therefore lacks the same risk of unintended second order consequences. This benchmark metric is contrasted with the approach of actors like Russia, which make

82 Klimburg, Alexander. "Mixed Signals: A Flawed Approach to Cyber Deterrence", Survival 62 (1), (2020): https://www.tandfonline.com/doi/abs/10.1080/00396338.2020.1715071?journalCode=tsur20.

83 Denver, James; Denver, Jack. "Cyber Realpolitik", Boston University Journal of Science and Technology v.21 (2019): https://www.bu.edu/jostl/files/2019/10/11.-Dever.pdf.

no such distinction and willingly employ disinformation and falsehoods to influence target audiences both in targeted operations and broad range STRATCOM, especially within social media.

The success of Glowing Symphony compared to the ineffectual STRATCOM efforts have informed future peacetime operations and doctrines, in which there are indicators that the U.S. prefers targeted information and cyberspace operations as a first response to nation-state adversaries in a peacetime environment.[84]These targeted countermeasures produce higher second-order normative effects in a peacetime setting than they do during wartime. The U.S. 2018 cyber doctrine delineates three components as part of its 'defend forward' posture: positioning, warning, and influencing. These trends, particularly the latter, have thus far raised concerns for the stability of the normative status quo, as the U.S. employs persistent engagement against peacetime nation state adversaries. The success of the kinetic cyber components of the counter-ISIS campaign contributed to this formulation of U.S. doctrine; the Wall Street Journal, quoting released government documents, states "lessons learned from Glowing Symphony helped influence the development of U.S. Cyber Command".[85]

By extension, the ineffectuality of U.S. strategic communication efforts to present an effective counter narrative to ISIS online hints at a rebalancing of preferences within U.S. thinking that threatens greater instability to the whole of the internet.[86] Notably, interdepartmental debates regarding Glowing Symphony, including "non-concurs" issued by officials, led to the Trump administration streamlining the ruleset governing offensive cyber engagement – another indication that the principle lessons of the ISIS case have been a more overt offensive U.S. strategic posture.[87]

In summary, the lessons learned from Glowing Symphony have informed an increased willingness to conflate cyber weapons with kinetic effects used in a wartime environment as an acceptable response to disinformation tools of influence in a peacetime environment, placing both at the same level and thereby fueling the Kremlin's *forever war* and *information warfare* narrative. This would risk bringing the U.S. into a more escalatory posture in dealing with disinformation and deviate from European thinking which prohibits such tactics during peacetime.

---

84 See countermeasures to Russian disinformation in the previous case study.

85 Volz, Dustin. "How a Military Cyber Operation to Disrupt Islamic State Spurred a Debate", The Wall Street Journal, (21 January 2020): https://www.wsj.com/articles/how-a-military-cyber-operation-to-disrupt-islamic-state-spurred-a-debate-11579604400.

86 Segal, Adam. "Cyber Week in Review: January 24, 2020", Council on Foreign Relations, (24 January 2020): https://www.cfr.org/blog/cyber-week-review-january-24-2020; Volz, Dustin: "How a Military Cyber Operation to Disrupt Islamic State Spurred a Debate", The Wall Street Journal (21 January 2020): https://www.wsj.com/articles/how-a-military-cyber-operation-to-disrupt-islamic-state-spurred-a-debate-11579604400.

87 Volz, Dustin. "White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons", The Wall Street Journal (20 September, 2018): https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729?mod=article_inline.

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