3. Case Studies of Norm Development in Hybrid Conflict

Summary

- This chapter applies the norm lifecycle to five cases to better understand the strategies, tools of influence, dilemmas and trade-offs by European states and the U.S. in their response to Russian and Chinese hybrid operations. These include (1) Russian cyberoperations; (2) Russian disinformation; (3) ISIS propaganda; (4) Chinese economic espionage; and (5) Chinese lawfare in the South China Sea.
- In the early stages of norm emergence, *linking* and *framing* are crucial tactical bargaining tools to persuade like-minded countries, complemented by *socialization* further down the norm lifecycle.
- Often the best path to support the acceptance of *existing* norms is to agree on *new* add-ons to reinforce existing ones as the norm to protect electoral infrastructure is seen as an enhanced interpretation of the existing norm on critical infrastructure protection.
- The development of norms may be better served when states mobilize coordinated large-scale attribution and subsequent sanctions *with* their partners specifically targeting norm violators instead of sweeping unilateral action.
- The analysis of the countermeasures against Russia's disinformation campaign suggests to *frame* a disinformation norm around covert election interference and *link* it to the non-intervention principle that prohibits concerted covert influence operations aimed at undermining democratic processes, while allowing overt support for democratic processes and voices.
- A normative benchmark for truthfulness in Western information operations is identified in which the broader the target audience and the mediums used (e.g. STRATCOM) the more truthfulness is prevalent, while targeted covert influencing operations (e.g. PSYOPS and MILDEC) may leverage a higher degree of falsehoods. This contrasts with the Russian Information Warfare approach, which makes no such distinction and willingly employs disinformation.
- When a state no longer pursues a persuasive strategy to push for norm acceptance, the target country may lose incentives for adherence, especially when this is replaced by a broader coercion strategy as indicated by the U.S. bilateral trade and tariff war targeting China.
- Seemingly internalized norms on freedom of navigation and innocent passage do not remain fixed or unchallenged. Chinese assertiveness in the South China Sea has not been effectively deterred by Western countermeasures, as Beijing continues to shape the contours and content of these norms.
- Finally, countermeasures can trigger second-order normative effects that are too often ignored. These are particularly risky 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.

The norm lifecycle is the theoretical basis through which we can now analyze norm development in five case studies to better understand the real-life strategies, tools of influence, dilemmas, and trade-offs that empower state-led norm processes. Throughout the case studies, the dynamics between countermeasures and norms are analyzed as part of the strategies adopted by the U.S. and European countries toward Russian and Chinese hybrid operations – with a primary focus on cyber and information operations, and a cursory glance at maritime operations.

The cases will identify the norms that the West seeks to promote through countermeasures against hybrid operations. The normative dimension of each case is analyzed at different levels. First, as previously described, states are aware that habit and repetition alone – especially when they go unchallenged – create norms. The countermeasures discussed in the case studies are aimed at derailing or delegitimizing unwanted Russian or Chinese behavior from establishing new norms. For example, U.S. countermeasures against Chinese cyber-enabled IP theft can be seen as denouncing and breaking a pattern of behavior that would otherwise normalize this form of economic espionage. Second, we assess whether the countermeasures reaffirm existing norms or whether they lead to the emergence of a new norm that shapes the behavior of the opponent. Third, if a new norm emerges, we assess its position within the norm lifecycle and identify the tools of influence used for cultivation. Finally, as states pursue what they may perceive as norm-enforcing behavior, their countermeasures may trigger second-order effects. These effects are often underestimated or even ignored when states consider their countermeasures, 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.

The selection of cases reflects the wide range of stages in the norm lifecycle. These encompass clear norm proposals that emerge from countermeasures with the intention to establish red lines for Russian and Chinese behavior (case studies 1 and 4). Herein, the application of the norm lifecycle showcases the strategic options and tools of influence that states can utilize. The application of the lifecycle is less straightforward when a norm has yet to emerge, when there is a norm conflict, or in times of war. Each scenario will be explored in more detail. In lieu of an explicit norm against disinformation, case study 2 offers guidelines for *framing* and *linking* a consensus norm in such a way that it prohibits concerted Russian covert disinformation campaigns while allowing Western overt influence tools. Because norms are primarily peacetime instruments, their application to military operations is limited, as shown in case study 3 dealing with U.S. countermeasures against ISIS propaganda. Instead, the case determines if the countermeasures occur in accordance with the principles of International Humanitarian Law. In comparing the Western approach to Information Operations with the Russian Information Warfare approach, the outset of a norm that

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

anchors truthfulness in the respective operations becomes visible. Finally, even norms that can be considered customary international law can be challenged. Case study 5 describes how Chinese claims and hybrid operations in the South China Sea undermine the established maritime norms of innocent passage and freedom of navigation.

Prior to the normative analysis, each case starts with a description of the hybrid operation, followed by the Western countermeasures and their underlying mandate. Herein, we use a broader interpretation of countermeasures than the strictly legal definition. Countermeasures encompass the broad range of state responses taken horizontally across the 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.[83] 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, case study 1 deals with diplomatic and economic countermeasures in response to Russian cyber operations, while the second case deals with more coercive military countermeasures, including offensive cyberspace operations, against Russian disinformation operations in peacetime. Case study 3 deals with the countering of propaganda within a conflict theater through information and cyber operations. Case study 4 and 5 deal with diplomatic and military measures against Chinese cyber-enabled IP theft and maritime operations in the South China Sea.

Structure of the case studies

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.

83 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.

3.1 Case 1: Protecting Electoral Infrastructure from Russian Cyberoperations

3.1.1 Incident

This case study focuses on the diplomatic countermeasures taken by the U.S. and European governments in response to Russian malicious cyber operations, as part of its larger hybrid campaign aimed at undermining international and democratic institutions and processes. The incident covered by the case study focuses primarily on the documented operations of APT-28 - aka *Fancy Bear* - between 2016 and 2018, which operated as part of Russia's GRU. This includes the hacking of U.S. and European political parties[84] and the attempted intrusion into national and international chemical organizations such as the Organization for the Prohibition of Chemical Weapons (OPCW).[85]

These operations place Russian doctrines of "active measures" and "reflexive control" within the context of cyberspace, in which strategic operations are planned and executed with psychological effects as the main underlying motivation. Russia's view of the importance of information as a weapon was clarified in the 2016 Information Security Doctrine, in which it distinguished two forms of informational attacks: a technical and a psychological attack.[86] It is mostly concerned with the latter, and nearly all technical attacks (including cyber and electronic attacks) are coordinated or supplemented with a psychological effect in mind. As such, the hacking of the U.S. Democratic National Convention (DNC) and the Clinton and Macron presidential campaigns led to the subsequent leaking of confidential documents, altered with fabricated information, amplified through Russian-aligned media outlets, such as RT and Sputnik, internet trolls, and co-opted sympathetic groups, like Wikileaks. The hack, therefore, allowed Russia to exploit existing societal differences, undermine Western democratic processes, and establish narratives in favor of the Kremlin.

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

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

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

3.1.2 Countermeasures

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

Public attribution and naming & shaming:[87]

In October 2016, the U.S. Department of Homeland Security and the Office of the Director of National Intelligence attributed in a general sense the "recent compromises of e-mails from U.S. persons and institutions, including from US political organizations" to Russia.[91] In July 2018, the U.S. government issued a more detailed account of hacking offenses related to the 2016 election in an indictment against Russian operatives.[92] In response to the Russian-orchestrated 'Macron Leaks' operation, it was easier for French officials to attribute the *disinformation campaign* to Russia because of the overt nature of parallel campaigns orchestrated by Russia Today and Sputnik. However, they never publicly attributed the *hack* to Russia.[93] Finally, the British response to the September 2018 poisoning of Sergei Skripal and subsequent Dutch response to the OPCW operation disclosed a high level of evidence,

Mandate Attribution: In the nation state context, public attribution, whether in the cyber or physical realm, is a political act based on sovereignty, and while there is no particular agreed upon standard of proof, countries still have a strong incentive to not make spurious allegations, lest they lose credibility.[88] Rather than employing collective or joint attribution, the EU's approach is predicated upon the principle that attribution is a political or sovereign decision made by the member states. It can be better described as coordinated among member states through information and intelligence sharing. Finally, it is important to note here that in the legal requirements for countermeasures as set forth by the International Law Commission in its Articles on State Responsibility, which generally reflect customary international law, the "injured" state's countermeasure must be intended to convince the "responsible" state to desist in its unlawful activities.[89] Countermeasures are, thus, subject to strict conditions, including the requirement that the injured state invokes the other state's responsibility. This involves the injured state establishing a violation of an obligation under international law that applies between the injured state and the responsible state and requires that the cyber operation can be **attributed** to the responsible state.[90]

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

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

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

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

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

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

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

including identities and personal data of the GRU officers they believed to be responsible.[94] A few days after the Dutch statement, the independent investigative collective Bellingcat, utilizing the published passports and information previously disclosed by the U.K. in response to the Skripal poisoning, exposed a major data breach disclosing the identities of approximately 305 GRU officers.[95] This proactive approach to naming and shaming had concurrent material and operational costs for Russia that neither the U.K. nor the Netherlands may have anticipated. It amounted to one of the few instances where naming and shaming served as an effective imposition of costs against Russia.

Diplomatic expulsions: Diplomatic expulsions go one step further in imposing costs on the perpetrator. The EU and its member states have made little use of indictments or sanctions in responding to malicious cyber operations thus far. Their use of public attribution contributed to a unified European response resulting in the expulsion of over 100 Russian diplomats by 19 EU member states and 10 other states, including the U.S. in March 2018, in response to the Skripal poisoning and the intended OPCW hack. As a response, the Kremlin escalated the crisis further when they decided to expel 40 American diplomats and close the American Consulate in St. Petersburg as a response, resulting in a further deterioration of U.S.-Russia relations.[96] Earlier, the U.S. undertook similar measures when it expelled 35 Russian diplomats for alleged interference into the U.S. presidential elections in December 2016.[97] Such a widespread expulsion of Russian diplomats had not occurred since the end of the Cold War. After threatening to retaliate in kind, Moscow eventually decided not to expel any diplomats, most likely because of U.S. presidential transition, which redirected the attention away from the hack while simultaneously offering an olive branch to incoming President Trump.[98]

Mandate Expulsions: A state can expel diplomats when they are considered "persona non grata", as defined under article 9 of the Vienna Convention Diplomatic Relations.[99] In this context, the diplomatic expulsion should be considered an act of *retortion*, an unfriendly but not unlawful measure that a state can take in response a similar act by another state's[100] Countermeasures are defined under international law as measures that would normally constitute a violation of an obligation under international law but which are permitted because they are a response to a previous violation by another state. They are subject to strict legal and political requirements, whereas retorsions can be taken at any time without taking these considerations into account as long as they are in line with their obligations under international law.[101]

94 Odell, Mark, "How Dutch Security Service Caught Alleged Russian Spies", Financial Times (2018): https://www.ft.com/content/b1fb5240-c7db-11e8-ba8f-ee390057b8c9.
95 Bellingcat Investigation Team, "305 Car Registrations May Point to Massive GRU Security Breach", (2018): https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/.
96 Higgins, Andrew, "Expelling Diplomats, a Furious Kremlin Escalates a Crisis", New York Times (29 March 2018): https://www.nytimes.com/2018/03/29/world/europe/russia-expels-diplomats.html.
97 Gambino, Lauren; Siddiqui, Sabrina; Walker, Shaun, "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking", The Guardian (2016): https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack.
98 Tamkin, Emily, "After Russians Promise Retaliation, Putin Decides Not to Expel U.S.", Foreign Policy (30 December, 2016): https://foreignpolicy.com/2016/12/30/after-russians-promise-retaliation-putin-decides-not-to-expel-u-s-diplomats/
99 Article 9 of the Vienna Convention: "The receiving State may at any time and without having to explain its decision, notify the sending State that the head of the mission or any member of the diplomatic staff of the mission is persona non grata or that any other member of the staff of the mission is not acceptable. In any such case, the sending State shall, as appropriate, either recall the person concerned or terminate his functions with the mission. A person may be declared non grata or not acceptable before arriving in the territory of the receiving State.", United Nations, "Vienna Convention on the Law of Treaties", (23 May, 1969): https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf.
100 International Law Commission, "Draft articles on responsibility of States for internationally wrongful acts, with commentaries", (2001) Yb ILC vol. II, Part Two.
101 Ministry of Defense of the Netherlands, "About the Netherlands Law Review", Military Law Magazine (2019): https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/.

Indictments: Within this case study, the U.S. took an assertive approach in its use of indictments. In July 2018, it indicted 12 Russian GRU officers for hacking the 2016 presidential elections - mostly targeting the DCCC and DNC networks, and the subsequent release of stolen documents.[102] It marked the first impactful acknowledgment and response from the Trump administration that a Russian government agency was behind the attack.[103] Following the public attribution of the Russian operatives behind the OPCW operation, the U.S. followed suit with indictments in October 2018, bringing charges against the GRU officers who were, amongst other things, involved in the OPCW operation.[104]

When Concord, a Russian company charged by the U.S. Mueller indictment, was the first to contest its charges in March 2020, the New York Times reported that "instead of trying to defend itself, Concord seized on the case to obtain confidential information from prosecutors, then mount a campaign of information warfare, a senior Justice Department official said."[105] As a result, the U.S. Justice Department dropped the charges to preserve national security interests and prevent Russia from weaponizing lawful protocols to acquire delicate American law enforcement information, according to the official. A guilty verdict against companies that cannot be meaningfully punished in the United States did not measure up against the risk of exposing national security secrets.[106]

Mandate Indictments: Bringing criminal charges in the form of indictments against foreign hackers differs from sanctions, expulsions or even military measures for responding to malicious cyber intrusions for two main reasons. First, criminal charges and indictments are carried out by law enforcement agencies to target individuals, rather than states, for criminal wrongdoing on the basis of domestic legislation.[107] Second, bringing criminal charges requires evidence that meets the requisites of probable cause by a grand jury or a judge in order to bring charges. This is in contrast to public state attributions where there is no evidence threshold and intelligence assessments may use classified sources and methods that may not be admissible in court.[108]

Sanctions: In December 2018, the U.S. Department of the Treasury imposed Russia-related sanctions, adding 18 Russians to their blacklist that were acting for or on

102 United States Department of Justice, "Case 1:18-cr-00215-ABJ Indictment", United States District Court for the District of Columbia, (2018): https://www.justice.gov/file/1080281/download.
103 Greenberg, Andy, "Trump's Win Signals Open Season for Russia's Political Hackers", WIRED (2016): https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/; https://www.wired.com/2016/11/trumps-win-signals-open-season-russias-political-hackers/.
104 United States Department of Justice, "U.S. Charges Russian GRU Officers With International Hacking and Related Influence and Disinformation Operations", Office of Public Affairs (2018): https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.
105 Benner, Katie; LaFraniere, Sharon, "Justice Dept. Moves to Drop Charges Against Russian Firms Filed by Mueller", New York Times, (2020): https://www.nytimes.com/2020/03/16/us/politics/concord-case-russian-interference.html.
106 *Ibid*.
107 In the U.S. case, the most cited legal basis for the indictments concerning malicious cyber operations derive from the Computer Fraud and Abuse Act: Doyle, Charles, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws", Congressional Research Service, (15 October, 2014): https://fas.org/sgp/crs/misc/97-1025.pdf; Johnson, Carrie: "U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports And Doping Groups", NPR (2018): https://www.npr.org/2018/10/04/654306774/russian-cyber-unit-accused-of-attacking-opcw-chemical-weapons-watchdog; United States Department of Justice, "U.S. Charges Russian GRU Officers With International Hacking and Related Influence and Disinformation Operations", (2018): https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.
108 *Ibid*.

behalf of, directly or indirectly, the GRU.[109] Amongst other allegations, they were found to be involved in hacking and meddling in the 2016 U.S. presidential election and against the OPCW. Consequently, any property or interests of these persons, subject to or transiting U.S. jurisdiction were blocked. The EU has thus far only used its recently acquired Cyber Diplomacy Toolbox once to adopt similar sanctions in response to Russian, Chinese and North Korean hacks, including the attempted hack against the OPCW.[110] Such a decision requires unanimity from all EU member states, which may make its use problematic considering some member states' entanglement with Russia on issues outside of the purview of this case study, such as energy dependencies, which may require them to adopt less coercive measures and seek cooperation and persuasion instead. This trend is indicated in the actions of German-French rapprochement towards Russia despite its information operations against both countries, [111] although increased pressure from the Dutch (and previously the UK) and more recently from the Germans has gone some way toward indicating a willingness to use sanctions against Russia.[112]

Mandate Sanctions: There is a large existing sanction framework in place at the UN, EU and national level that can be imposed against states, organizations, and persons encompassing financial sanctions (asset freezes), trade embargoes (flight and shipping bans or export limitations), arms embargoes (prohibition of weapon and dual-use exports), and travel restrictions (visa bans). Both within the EU and the U.S. context, sanctions targeting malicious cyber operations are primarily directed at persons or organizations rather than states. In the US, the Treasury Department is the agency and does so based on Executive Order 13757 and 13694 that specifically deal with cyber-enabled activities, as well as pre-existing sanction statutes and regulations.[113] The Russian operatives sanctioned by the U.S. were done pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA).[114] The EU endorsed its sanction regime to counter malicious cyber operations in June 2017 through the so-called Cyber Diplomacy Toolbox.[115] It is coordinated by the European External Action Service and includes restrictive measures for individuals and other entities, such as asset freezes and travel bans.

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

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

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

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

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

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

115 Council of the European Union: "Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States" EUR-LEX Document 32019R0796 (2019): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.ENG&toc=OJ:L:2019:1291:TOC.

In summary, the countermeasures described eliminate the secrecy surrounding cyber operations and may serve to rebalance the cost-benefit calculations of future hybrid aggressors, as their operations illicit economic sanctions and legal indictments which raise the cost of their activity. Additionally, the largescale GRU data breach highlights the effectiveness of attribution as a form of punishment and the risk of unanticipated consequences of hybrid action, where previously they may have been viewed as a low-cost alternative to direct confrontation. The countermeasures employed by the U.S. and EU states reflect differences in capabilities, vulnerabilities, and their overall guiding doctrines in responding to a mutual problem. The constraints of political coordination amongst EU member states to use coercive tools, the relatively young mandate to use them, and mutual dependencies with Russia restrict Europe from embarking on the same coercive measures – such as sanctions and indictments – undertaken by the United States. Alternatively, proactive U.S. countermeasures may be viewed as a means to compensate for its relatively weak resilience[116], whereas the EU and its member states focus on their relatively better resilience posture supplemented by less coercive countermeasures, such as naming and shaming.[117] These realities inform the preference of methods by which both actors formulate their strategic postures, including the use of countermeasures. The following section extrapolates these measures in terms of their influence over emergent norms, and their second-order impacts upon the wider body of established and internalized norms.

3.1.3 The Normative Dimension: What Norms are Promoted?

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

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

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

result from the countermeasures that may conflict with the European and American long-term interests and counter-hybrid posture.

Affirmation of Existing Norms?

Despite differences in their escalation posture, one could argue that both the U.S. and European responses indicate a commitment to reaffirm the existing norm prohibiting cyberattacks against critical infrastructure from the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which is broadly adopted by all members of the UN General Assembly. The norm, however, does not specify what constitutes critical infrastructure. While the U.S. and several of its European counterparts may label electoral infrastructure as critical, Russia may not. While the countermeasures may indirectly link to the respective norm, the commitment remains circumstantial at best and could be improved through specifying the exact norm violations by Russia. Should states decide to *link* to the norm violation in their response, norm adherence and accountability is improved through reaffirmation. If this is not done, countermeasures risk challenging or even violating established norms. This risk is further exacerbated by the U.S. persistent engagement doctrine that allows for a more offensive cyber posture, which is explained in more detail in case study 2. Whilst some might argue that the routine violation of ostensibly internalized norms by states like Russia could undermine these efforts, countries like the U.S. and its European counterparts have worked to build support for its condemnations of their activity amongst allies and other nations. If there is no response regardless, states risk normalizing malicious behavior through tacit acceptance.[118]

A New Norm Emerges?

Alternatively, one could argue that the record of public attributions, indictments, sanctions and diplomatic expulsions contributed to the emergence of a new norm to protect electoral infrastructure from cyber operations. By labeling specific infrastructure such as electoral systems as critical, the norm creates an enhanced interpretation of the GGE norm on the protection of critical infrastructure. Academic research has shown that it can take years for norms to be commonly adhered to and that often the best path to support the acceptance of existing norms is to agree on new add-ons to reinforce existing ones.[119]

---

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

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

Norm Emergence: Framing and Linking

The explicit norm proposal to protect electoral infrastructure originated in 2018 from the Global Commission on the Stability of Cyberspace (GCSC)[120], a transnational civil society-led initiative, and was later adopted by the Paris Call for Trust and Security in Cyberspace – a high-level declaration of French President Macron with over 1,000 state, industry and civil society signatories, but excluding Russia, China and the United States.[121] Given that the norm is relatively new, it is best categorized within the early stages of its lifecycle: norm emergence. The main actors in this case are the *norm entrepreneurs* that can create or leverage influence in *organizational platforms* to convince a critical mass of actors to embrace the new norm in its early stages by *framing* it within a particular context that works favorably to the interests of the entrepreneur and by *linking* it to other impactful issues that attract attention and resources.

The entrepreneurs, in this case, initially the GCSC and later the French government (the main actor behind the Paris Call) and Dutch government (advocated for the norm in the UN), *frame* the norm within a particular context, thereby shaping the identity of the players affected by the norm. In contrast to the norms developed within the interstate UN context, this particular norm puts the onus not only on states but also on non-state actors, thereby extending its applicability to proxy actors. In terms of the prescribed behavior, the norm can be considered regulative, prohibiting offensive cyber operations from targeting the technical infrastructure essential to elections, referendums or plebiscites, while it excludes the contentious issue of content or disinformation. Such offensive operations are framed as a threat to democracy by *linking* it to the principle of non-intervention enshrined in article 2(4) of the United Nations Charter, explaining that elections lie at the heart of sovereignty, territorial integrity and political independence.[122] While the norm did not utilize naming and shaming tactics or accused actors explicitly, it was proposed at a timely moment, just after the described incidents of this case, and linked the norm to the growing number and intensity of threats to participative processes, and recognizing that such attacks are unacceptable.[123]

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

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

122 Article 2(4) of the UN Charter states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations": https://www.un.org/en/sections/un-charter/un-charter-full-text/.

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

Socialization

Using the Paris Call for Trust and Security in Cyberspace, linked directly to the Paris Peace Forum and indirectly to Internet Governance Forum, as an organizational platform, France managed to *socialize* its emerging norm entrepreneurship within a large group of like-minded countries, as well as industry and civil society. While a large majority may subscribe to the norm because they agree with the content, others may have acted more strategically by adopting the emergent norms to avoid stigmatization without the intention of actually upholding its principles – a form of social camouflage through false-positive. This is especially effective in tight-knit groups, such as EU member states, wherein they are concerned with their reputations within their specific community. After all, conformity to the Paris Call improves the reputation of a state as a responsible actor as it operates as a public member of its community. This is especially the case when a norm entrepreneur uses organizational platforms to institutionalize the norm. This could in turn contribute to a dynamic of imitation and bandwagoning as norm leaders attempt to socialize other actors to become norm followers. This was reflected by the near threefold growth of total subscribers to the Paris Call, of which state parties grew from just over 50 to 70.[124] When it comes to the effect of socialization in relation to Russia, the tool of influence is limited to *stigmatization* as Russia, along with the U.S. and China, did not sign up for the Paris Call. This stigmatization is enhanced by more coercive socialization tools, such as public attribution or naming and shaming.

Through its active advocacy functions, both the GCSC and the Paris Call acted as organization platforms that created diplomatic momentum and leverage for states, most notably France and the Netherlands, to socialize the norm among state actors within the United Nations Open-Ended Working Group (OEWG) in the Field of Information and Telecommunications in the Context of International Security.[125] It did so by linking it to the pre-existing critical infrastructure as critical; the norm thus creates an enhanced interpretation of the GGE norm on the protection of critical infrastructure.

Persuasion

In terms of persuasion, the norm entrepreneurs used framing techniques in addition to linking the norm to other powerful pre-existing norms to increase its credibility and urgency. While like-minded countries within the OEWG would rather focus on promulgating already established norms, rather than adopt new ones, this norm is *framed* as being an expansion to a pre-existing norm established by the GGE on the protection of critical infrastructure. This *links* the argument to the fact that multiple

124 Paris Call, "For Trust and Security in Cyberspace", (11 November, 2018): https://pariscall.international/en./

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

countries, such as the U.S., have already internalized their norm in national legislation by considering electoral infrastructure as critical and thus requiring merely the extension of existing standards, rather than the formulation of entirely new norms.

In terms of positive inducements or material incentives, there are few overt measures that are directly linked to the promotion of the norm. One exception may be the capacity building partnerships between industry and civil society within the context of the Paris Call created, such as the initiative from Microsoft – the industry partner for the Paris Call - and the Alliance for Securing Democracy partnership to prevent malign interference by foreign actors.

Coercion

The third tool used to promote the norm - *coercive strategies* – reflects the previously described countermeasures adopted by the U.S. and its European counterparts towards Russia. These include the use of *coercive socialization* through naming and shaming by the U.S. in response to the hacking of the DNC. Whereas the French government did not officially attribute the *hack* of the Macron campaign (in contrast to the disinformation campaign that was officially attributed), private cybersecurity companies, such as Trend Micro did attribute the hack to the GRU.[126] Diplomatic expulsions, indictments and sanctions were used by the U.S. in response to the interference of the U.S. presidential elections and the hacking of the DNC. The details of these events are explained in the first section of the case study. The sanctions and indictments were justified on the basis of national U.S. mandates and legislation, showing that the U.S. internalized the norm within its policies. While these measures were directed at imposing costs, they also shape the behavior of Russia by drawing a red line and reaffirming a norm that goes against the targeting of electoral infrastructure.

In conclusion, whilst the norm against cyber operations targeting electoral infrastructure is in its early stages of the lifecycle, the strategies and tools of influence used by the entrepreneurs can be described as pluralistic, meaning that they intend for the norm to be spread and internalized using multiple influence strategies simultaneously – through both words and action. In its early stages, multiple state and transnational NGO entrepreneurs *persuade* others by *framing* the norm to larger issues such as the threat to democracy and sovereignty from malign state and non-state actors, and by *linking* it to well-established norms on non-intervention and critical infrastructure protection. This can be further enhanced through capacity building initiatives and other positive inducements linked to the norm. The entrepreneurs have thus far used organizational platforms such as the GCSC, Paris Call, and the UN, to socialize the norm with both state and non-state actors. While most like-minded countries, such as the US, prefer

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

to focus on implementing previously agreed GGE norms over creating new norms in the UN, the auspicious entrepreneur not only links the norm to these GGE norms but frames it as an enhanced understanding of them. Furthermore, the U.S. diplomatic countermeasures against Russia can be considered an *internalization* of the norm prohibiting cyber operations against electoral infrastructure. The socialization effects of the norm on Russia and China, however, is limited to stigmatization, naming and shaming, and more coercive tools, such as sanctions and indictments.

Second-Order Normative Effects of the Countermeasures

States may underestimate or even be unaware that countermeasures may establish new norms that conflict with their own long-term interests. As these norms are in their early emergence, they, and the countermeasures which initially formed them, may produce unanticipated long-term consequences. We will take a closer look at how these effects impact the long-term interests of the states that undertook the countermeasures and the normative initiatives of their opponent. In this case study, we identify three negative externalities associated with the respective countermeasures that are not prohibitive but should be taken into consideration as they have an impact on the development of international norms and could run contrary to the interests of the entrepreneur. These include the effects of attribution on the existing norms or standards of proof and on prohibiting intelligence operations that are not prohibited under international law, and finally the effects of the politicization of indictments on lawfare.

Highly detailed public attribution can set a precedent for a high standard of proof. Although the EU Cyber Diplomacy Toolbox and indictments require an evidence threshold, there is no standard of proof for public attributions by states. Previous public attributions did not disclose a high level of detail regarding the perpetrators, their tools, or the attack vector due to fear of losing intelligence assets. It would provide a glimpse at their operational tools, techniques and methods used to attribute the attack. At the same time, Moscow's rejection of this kind of public attribution is usually based on the lack of evidence provided by the victim state – thereby placing a burden of proof upon the victim at their own cost. This case, however, sets a precedent for highly detailed disclosures that eliminates this plausible deniability of the perpetrator and consequently reveals their techniques, tactics and procedures (TTPs), leading to a more convincing message towards allies and the general public. While this is a largely positive development that does not constitute an explicit effort to establish a new norm on standards of proof, the action and subsequent public attributions of Russia's actions and GRU cyber operations in such recent cases as in Georgia,[127] may inherently contribute to the Russian narrative that a certain burden of proof is required by the victim.

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

A lack of clarity about the nature of an incident and the basis of a response can establish a norm against intelligence operations. Aside from the norm setting in terms of *how* states conduct attribution, the response to the OPCW operation reveals something about the kind of behavior it tries to punish. Because offensive cyber operations are preceded by intelligence operations, it remains very difficult to discern the true intention behind an intrusion: is it an intelligence operation, signaling, or preparation of the battlefield? In the Dutch press release following the foiled OPCW hack, the case was considered digital manipulation and sabotage, while others consider it to be an intelligence operation – something that is not explicitly prohibited under international law.[128] If the Russian operation did not violate an international norm or law, is the Dutch response setting a norm against intelligence operations? This remains unlikely, partly due to Dutch self-disclosures about its own security and counter-intelligence operations against the GRU, and partly because it did not take additional further-reaching measures than expelling the Russian operatives. Instead, the GRU officers were indicted by the US. Unless it was contributing to the further blurring between what constitutes acceptable and non-acceptable behavior in cyberspace, the goal of this countermeasure was not to indicate if Russia violated a norm, but to mobilize a broader diplomatic confrontation. As an aspect of the norm lifecycle, this prudence reflects the complications of delineating 'conventional' intelligence operations from the more egregious forms of hybrid meddling perpetrated by Russia. Existing trends amongst victim states show a habit of linking attack vectors to aspects of national security as a means of framing countermeasures; in this way, victim states are demonstrating an effort to define in normative terms the parameters of 'unacceptable' hybrid warfare, as opposed to an accepted form of intelligence gathering.

Politicizing indictments can escalate lawfare. The use of indictments can reinforce existing norms but does not come without risks and possible criticism. Criminal charges are usually processed independently from political considerations. Russia has weaponized this argument by claiming that the U.S. indictments are simply political actions.[129] It hinted at politicization when Concord, a Russian company charged by the U.S. Mueller indictment, was the first to contest its charges in court. In March 2020, The New York Times reported that "instead of trying to defend itself, Concord seized on the case to obtain confidential information from prosecutors, then mount a campaign of information warfare, a senior Justice Department official said." As a result, the Justice Department dropped the charges to preserve national security interests

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

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

and prevent Russia from weaponizing lawful protocols to acquire delicate American law enforcement information, according to the official This also ties into the broader concern of Western countries about the politicization of international law enforcement efforts and initiatives - a form of lawfare by countries like Russia and China.[130] These adversaries may therefore act more aggressively and freely to politicize international law enforcement as a response and in an effort to undermine cooperation on common issues unaffiliated with inter-state hybrid warfare (i.e. combatting cybercrime). As a reflection of norm development, an increase in lawfare between states through international institutions would significantly challenge norms on multilateral cooperation in cyberspace.[131]

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

3.1.4 Key Takeaways

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

The norm moves from emergence to cascade and internalization. Taking into consideration its short lifespan, the norm has already cascaded to a high degree of parties through organizational platforms, and is already being internalized as states, especially powerful norm leaders like the U.S., are categorizing electoral infrastructure

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

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

as part of their critical infrastructure and take coercive measures to enforce the norm. For now, the socialization effects of the norm on Russia and China, however, is limited to stigmatization, naming and shaming, and more coercive tools, such as sanctions and indictments, which are harder to combine with the other tools of influence. As of now, the norm is included in the pre-draft report of the UN OEWG.[132] Adoption within the UN would constitute a major socialization effect across states, moving beyond norm cascade, and intensifying the internalization process. One could argue that Russia's commitment to the norm is insincere, but it then faces a choice between doubling down on hypocrisy or shifting its behavior in accordance with the norm. Positive inducements, such as capacity building, can be used to accelerate internalization of the norm, and coercive methods can be used to punish transgressors.

States should be aware of the normative second-order effects of attribution and indictments. Norm-setting by countermeasures can have unintended second-order effects, where a state creates a new norm through its countermeasure that may not be in its own strategic interest. Detailed disclosures of evidence in public attributions, whilst good for transparency and eliminating plausible deniability, may be grist to the mill of the Russian narrative that wishes to introduce a standard of proof for public attributions by states. The perceived politicization of indictments may have the same second-order effect on lawfare between states, thereby undermining the norms and rules tied to these platforms as they become embroiled in lawfare. By obfuscating between intelligence and cyberattack operations, a state may also contribute to the further blurring between what constitutes acceptable and non-acceptable behavior in cyberspace. Consequently, intelligence agencies may assume the role of norm entrepreneurs – setting the standards of tolerable conduct in cyberspace for the rest of the international community whilst remaining under the radar of international regulation as sub-state actors.[133] The risks of these normative second-order effects can, and have been, to a large extent mitigated through clear diplomatic engagement. This is not the case for the effects resulting from further-reaching military or kinetic countermeasures described in the next case study.

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

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

3.2 Case 2: Responding to Russian Disinformation in Peacetime

3.2.1 Incident

Whereas the previous case study focused on Russia's hacking, this case study takes a closer look at Russian disinformation campaigns, such as those executed by state-sanctioned 'troll factories', the principal example of which is the Internet Research Agency (IRA). The U.S. was targeted by Russian campaigns both in its 2016 Presidential elections and subsequent 2018 midterm elections, constituting a serious challenge to the democratic integrity and processes of many Western countries. The most documented campaign is referred to as 'Project Lakhta' – a Russian state-sanctioned umbrella effort that used disinformation to target domestic audiences within Russia, the U.S., EU member states and Ukraine.[134] According to the U.S. Department of Justice, it operated a $35 million budget between January 2016 and June 2018, of which the last half-year constituted $10 million.[135] The Russian operatives went to extraordinary lengths to mask their location and appear as American political activists on social media platforms to create and amplify divisive social and political content and to advocate for the election or electoral defeat of particular candidates in the U.S. and European elections. Some social media accounts posted tens of thousands of messages and had tens of thousands of followers.[136] These efforts which co-opted or manufactured echo-chambers through such platforms as Russia Today (RT), Sputnik, and alt-right platforms, aimed to utilize disinformation to exacerbate existing political polarization and consequently influence the U.S. 2016 Presidential and 2018 midterm elections, as well as those of European states, such as the United Kingdom, Germany, and France.[137] Within the European context, this case will focus on the 2017 French presidential election, in which Emmanuel Macron's campaign suffered a similar Russian-orchestrated disinformation campaign – albeit with a much lower degree of success than in the United States.

3.2.2 Countermeasures

In responding to similar threats of Russian electoral interference, the United States and France deployed markedly different countermeasures. France largely relied on tested information security practices to slow down the attacker and engaged in a proactive debunking of disinformation, reserving its countermeasures to diplomatic

134 US Department of Justice, "Russian National Charged With Interfering in U.S. Political System", Press Release (19, October, 2018): https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system.
135 *Ibid*.
136 Nahzi, Fron, "The West Cannot Sit by While Russia Exploits Social Media with Disinformation", The Hill (26, December, 2019): https://thehill.com/opinion/international/475797-the-west-cannot-sit-by-while-russia-exploits-social-media-with.
137 Intelligence and Security Committee of Parliament, "Russia", Government of the United Kingdom (21 July 2020): https://int.nyt.com/data/documenttools/intelligence-and-security-committee-s-russia-report/9c665c08033cab70/full.pdf.

statements and name-and-shaming of Russia's malign behavior. By contrast, the U.S. embarked on an aggressively offensive strategic posture, combining sanctions and indictments with the shutting down of one of Russia's primary "troll factories" for a number of days during the U.S. midterm elections in 2018, and publicly revealing a pre-deployment of cyber weapons within Russia's critical infrastructure as means to convey deterrence by punishment via coercive signaling. The U.S. countermeasures to Russian disinformation relied on several actions, including public attribution, indictments and sanctions, similar to those described in the previous case, that were issued against the IRA and other involved Russian companies such as Concord, as featured in the Mueller Report in 2018.[138] Since these measures and their underlying mandate were already described in the previous case, this case will focus more on the coercive proactive countermeasures employed by the U.S. against Russia: the shutdown of the IRA.

U.S. Cyber operation against the Internet Research Agency: In February 2019, it was reported that U.S. CYBERCOM had hacked and shutdown the Russian IRA in November 2018 'for a number of days' as part of *Operation Synthetic Theology* in order to safeguard the U.S. midterm elections.[139]

Mandate Offensive Cyber Operations (U.S.): The domestic legal basis for U.S. cyber operations is under the National Defense Authorization Act and revised 10 U.S.C. § 394, which expanded the authority of the Defense Department to operate in the cyber domain including operations "short of hostilities" and those "in areas in which hostilities are not occurring".[140] It emphasizes cyber operations as being a component of traditional military activity, for the purposes of attaining legal status as covert action – a traditionally vague area of international law may or may not consider such activities as falling under "countermeasures".[141]

U.S. Pre-deployment within Russian critical infrastructure: The United States response supplemented its initial cyber sabotage of the troll factory with a leaked report on its "pre-deployment" of cyberweapons in the Russian power grids, likely similar in scope to the reported Russian 'DarkEnergy' cyberweapon deployment in the U.S. and elsewhere.[142] Rather than 'allowing' their own pre-deployment operation to be discovered and reported by Russian actors, the U.S. self-disclosed that since 2018 they had implanted malware within Russian critical infrastructure in order to affect a kinetic-equivalent strike, if necessary.[143] The intent

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

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

140 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.

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

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

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

Mandate U.S. Pre-deployment: The doctrinal mandate for the U.S. countermeasures derives from its doctrine of 'defend forward' and 'persistent engagement'.[145] Enshrined under the 2019 National Defense Authorization Act, this mandate approves the routine conduct of "clandestine military activity" in cyberspace, to "deter, safeguard or defend against attacks or malicious cyberactivities against the Unites States [...] before they reach their target", through continuous engagement, contestation and confrontation of adversaries throughout cyberspace that causes uncertainty wherever their adversary maneuvers.[146] Ultimately, this would allow the U.S. to gain operational advantages whilst denying them to adversaries.

Mandate Offensive Cyber Operations (France): In the context of international law, the 2019 Ministry of Defense "International Law Applicable to Operations in Cyberspace" formulates that France may respond diplomatically, by way of countermeasures, or employ its armed forces to repel an armed attack.[149] This constitutes the legal basis for France's adoption of "active defense"[150], which is in line with its White Papers[151] (the 2017 "International Cyber Strategy"[152], 2018 Strategic Review of Cyberdefense"[153]) and their statements within the United Nations. The term "active defense" is encompassed in the *National Defense White Paper of* 2008; it denotes a "transition from a passive defense strategy to an active defense strategy in depth, combining intrinsic protection of systems, permanent surveillance, rapid reaction and offensive action."[154]

of this disclosure amounted to a display of coercive signaling to the Russians that the U.S. was ready to accept a level of 'mutually assured disruption'.[144]

French diplomatic signaling: The French response to a similar Russian disinformation campaign launched during its 2017 presidential election kicked-off with a clear signal from the French government – both publicly and through confidential channels – that it was determined to prevent, detect, and if necessary, respond to foreign interference. In a speech in December 2016, Minister of Defense Jean-Yves Le Drian announced the creation of a cyber command composed of 2,600 "cyber fighters".[147] A few weeks later, the minister publicly remarked that "by targeting the electoral process of a country, one undermines its democratic foundations, its sovereignty" and that "France reserves the right to retaliate by any means it deems appropriate through our cyber arsenal but also by conventional armed means."[148] Although the promise of a "retaliation by any means" never materialized – at least not in an explicitly escalatory manner – the French managed to respond effectively to the Russian disinformation threat through their preparedness and ability to a whole-of-society response that included timely and coordinated joint efforts from government and media institutions.

144 Maker, Simran, "Mutually Assured Disruption – Report", (12 January, 2018): https://www.ncafp.org/12606-2/.
145 United States Department of Defense: "Cyber Strategy 2018", (2018): https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.
146 Thornberry, Mac. "Text - H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019." (August 13, 2018): https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
147 Delerue, François; Géry, Aude, "The French Strategic Review of Cyber Defense", ISPI (2 May, 2018): https://www.ispionline.it/it/pubblicazione/french-strategic-review-cyber-defense-20376.
148 Conley, Heather, "Electoral Interference", CSIS Briefs (21, June, 2018):: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.
149 Roguski, Przemyslaw, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I", OpinioJuris (24, September, 2019): http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.
150 Roguski, Przemyslaw, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, PartII", OpinioJuris (24 Septmber, 2019): https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-ii/.
151 Ministry of Defence France, "Defense and National Security White Paper", (29 April, 2013): http://www.livreblancdefenseetsecurite.gouv.fr/.
152 Ministry for Europe and Foreign Affairs of France: "Stratégie Internationale de la France pour le Numérique", Diplomatie: https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.
153 Secretariat-General for National Defence and Security of France, "Revue Stratégique de Cyberdéfense", Government of France (2018): http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.
154 Baumard, Philippe, "Cybersecurity in France", Springer Briefs in Cybersecurity, (2017): http://www.idemployee.id.tue.nl/g.w.m.rauterberg/amme/Baumard-2017.pdf.

French information security and debunking: The Macron campaign enacted tested information security practices, including the placing of honeypots, false flags and forged documents under the pretense that they would be hacked, thereby inundating, confusing and slowing the attackers.[156] Given the tight timeframe of the elections, these measures were especially effective. The Marcon team communicated openly and extensively about the hacking and disinformation operations, gained control over the leaked information through the forged emails that they placed in honeypots, and actively debunked disinformation on social media to control the narrative. These debunking initiatives were not isolated to the Macron campaign team but collated around several independent researches and reliable media sources who conducted fact-checking of rumors leveled at Macron, largely from his opponent Marine Le Pen.[157] Some fake emails were so obvious that they actually helped the Macron team debunk the leaks as disinformation.[158] Furthermore, on the night of the disinformation dump, the Macron team informed the CSA, the French regulatory media authority, who asked all major news outlets to abstain from disseminating the false news. The team also informed the CNCCEP, the French electoral authorities, which issued a press release the following day asking "the media not to report on the content of this data, especially on their websites, reminding the media that the dissemination of false information is a

Mandate Anti-disinformation: The French disinformation law, which aims to better protect democracy against the different ways in which fake news is deliberately spread, was approved in its second reading at the National Assembly on 20 November 2018. The law places special attention on the spread of disinformation during elections based on the legal definition of *fake news*, as defined in the 1881 law on the freedom of the press, in accordance with three criteria: "(i) the fake news must be manifest, (ii) be disseminated deliberately on a massive scale, (iii) and lead to a disturbance of the peace or compromise the outcome of an election". Compliance to the law will be enforced by the French Broadcasting Authority, the CSA, which is able to "prevent, suspend and stop the broadcasts of television services that are controlled by foreign states or are influenced by these states, and which are detrimental to the country's fundamental interests."[155]

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

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

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

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

breach of the law, above all criminal law."[159] The majority of traditional media abstained from publishing about the leaked documents or urged their readers to be cautious about the leaked documents. As a result, there was no information laundering, nor whitewashing or mainstreaming of the disinformation. Instead, the French population doubted the authenticity of the leaked documents and they generated relatively little traction compared to the United States.

Focused more on the combination of preventive cyber resilience and active debunking of disinformation than offensive engagement, the co-opting of the mainstream media by the Macron campaign and French institutions stigmatized Russia's actions and those of their collaborators, going as far as to threaten legal repercussions to outlets considering publishing the leaks.[160] The campaign decided to deny Russia Today accreditation to cover the remainder of its campaign.[161] The reason cited was their "systematic desire to issue fake news and false information" as well as their "spreading of lies methodically and systematically."[162] This is also the position the European Parliament adopted as early as November 2016.[163] Even after the election, Russian outlets have been occasionally banned from presidential and Foreign Ministry press conferences justified on the basis that these are propaganda entities and not media outlets as President Macron publicly stated following his meeting with Putin at Versailles only weeks after his election.[164] In July, 2020 Latvia's national media watchdog, the Electronic Mass Media Council (NEPLP), banned Russia Today, citing it as a propaganda outlet.[165]

***Mandate Active Defense*:** The doctrinal underpinnings of France's strategic mandate are difficult to ascertain as they largely defaulted to ad hoc adaptations to the evolving scope of Russian activities. The policy of "active defense" has subsequently framed the formulation of French doctrine, in tandem with its continued policies of stigmatization and bilateral diplomatic engagement with malign state-sponsored hybrid actors. France draws a clear separation between offensive and defensive cyber operations and isolates its cyber defense agency from its wider intelligence apparatus.[166]

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

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

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

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

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

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

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

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

Taken together, the French response successfully mitigated Russian strategic aims despite the widespread incitement of a disinformation campaign, data hacking, and large-scale leaking; there was no whitewashing or mainstreaming of the leaked data by the professional media. In contrast to the hands-off posture of the U.S. government in the 2016 Russian electoral interference, three French administrative bodies took the lead in bolstering the Macon campaign's response by offering politically neutral expertise on dispelling Russian disinformation. These were the Constitutional Council, which represents the electoral judge and body in charge of electoral integrity; the National Commission for the Control of the Electoral Campaign for the Presidential election, a campaign watchdog; and, the National Cybersecurity Agency, which operates under the Prime Minister.[167] Through these efforts, the French government successfully prevented the final stages of election meddling: there was no 'information laundering', nor mainstreaming or whitewashing of the disinformation, the process by which traces of foreign interference are removed from the information narrative. As respective approaches to a mutual problem, the U.S. and French represent archetypes of alternative doctrines, specifically in their divergence along lines of "persistent engagement" versus "active defense".

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

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

3.2.3 The Normative Dimension: What Norms are Promoted?

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

Affirmation of Existing Norms?

Sovereignty. Some may believe that the principle of sovereignty already erects a normative barrier to Russia's disinformation efforts. In its response, France linked the disinformation campaign to the norm of sovereignty, stating that "by targeting the electoral process of a country, one undermines its democratic foundations, its sovereignty".[168] In addition, the specific ruling that "the principle of sovereignty applies to cyberspace" equates sovereignty in cyberspace with traditional notions of territorial sovereignty, the use of force, and non-intervention by one state into the territory of another.[169] Within the cyber context, there remains an ongoing debate as to whether sovereignty itself is an enforceable rule of international law or merely a principle of international law.[170] France is among the former group and holds that "any unauthorized penetration by a state into French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty".[171] Austria, Germany, the Netherlands and the Czech Republic also agree with the sovereignty-as-a-rule interpretation, albeit with varying degrees as to what kind of activity would automatically constitute a violation of sovereignty. By contrast, the U.S., like the U.K., holds the view that sovereignty is merely a principle of international law and does not create autonomous and separate legal obligations, but is protected by other established rules of international law, such as the prohibition of

168 Jean-Yves Le Drian (minister of defense), interviewed in Le Journal du Dimanche, "France Thwarts 24,000 Cyber-Attacks Against Defence Targets", BBC, (8 January, 2017): https://www.bbc.com/news/world-europe-38546415.
169 Ministére des Armées, "International Law Applied to Operations in Cyberspace": https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf#page=6.
170 Roguski, Przemyslaw, "The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States", Just Security (11 May 2020): https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.
171 Ministry of Defense France, "International Law Applied to Operations in Cyberspace": https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf#page=6.

the use of force or the principle of non-intervention.[172] Without going into the legal details of this debate, it is clear that the principle of sovereignty would offer little relief by itself — the purported rule suffers from much ambiguity with respect to state cyber and information operations.[173]

Nonintervention. Article 2(4) of the United Nations Charter articulates the nonintervention rule and elevates it as a principle of legal, and thus, binding character.[174] Whereas the norm proposed in the previous case study was linked to article 2(4) through the prism of cyberspace, this case study analyzes it through the prism of the information environment.[175] Article 2(4) of the UN Charter states that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[176] Traditional understandings link the prohibition on the use of force to an element of armed force involved, or at least actions resulting in physical injury or damage. Russian hybrid operations exploiting the gray zone have generally sought to test the response thresholds of their opponents and steer clear of causing physical harm, at least in the cyber and information environment, and thereby from tripping over the use-of-force threshold.

Cyber operations can reach the threshold at a loss of life and significant economic harm, which has been reaffirmed by a growing number of states, including the Netherlands and France.[177] States, however, have been less open about the application of this threshold to disinformation – a form of statecraft not prohibited under international law. They have not and are unlikely to deem Russia's spread of disinformation as a use of force. Doing so would mean that they agree with the Russian and Chinese

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

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

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

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

176 *Ibid.*

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

interpretations of use of force that includes psychological and media warfare.[178] Russia's and China's perceptions of information as a weapon consider bad *content* as critical or dissenting of the regime and thereby as an attack against the state.

The principle for nonintervention in the internal affairs of other states is, however, well-established within customary international law. It allows states to safeguard their sovereignty and independence, and its application to cyberspace has been established and reinforced by many states.[179] Like the use-of-force prohibition, the nonintervention rule is considered to be of limited scope. Fundamentally, it prohibits the use of *coercive* measures to overcome the free will of a targeted state with respect to matters that fall within that state's core, independent sovereign prerogatives.[180] "Unfortunately, the concepts of coercion and "domaine réservé"—the bundle of sovereign rights protected by the rule—are ill defined".[181] Such ambiguities can be cleared up by states disclosing their official views and interpretations. Thus far, only a handful of states have done so on the application of the nonintervention rule in cyberspace and even less for the information environment. The most concrete statements that go beyond a general acknowledgment that the parameters of the rule 'have not yet fully crystallized in international law' is the manipulation of electoral processes and the COVID-19 *infodemic*.[182] The United Kingdom goes further in its statement that an intervention in the fundamental operation of Parliament or in the stability of the financial system would "surely be a breach of the prohibition on intervention."[183]

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

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

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

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

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

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

Arguably, disinformation campaigns that aim to sow discord, distrust, and societal division do not instantly lead to a conclusion of *coercion* as individuals are free to accept and reject information they come across. Nonetheless, the national mandate for the countermeasures described earlier can provide guidance to the clarification of the coercion element. By linking Russian disinformation in 2016 to fraud and deceit, Special Counsel Robert Mueller's indictment demonstrates that covert deception and disinformation can be just as harmful to sovereign prerogative as more overt coercive measures, if not more so.[184] It also reinforces that election processes are a paradigmatic example of the type of sovereign prerogatives protected by the nonintervention rule, leading some legal experts to assert that Russia's election interference crossed a red line.

A New Norm Emerges?

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

Linking disinformation to the nonintervention principle. The principle of sovereignty offers a good starting point but little relief by itself given the ongoing debate as to whether sovereignty itself is an enforceable rule or merely a principle of international law. Instead, election meddling is one of the few forms of disinformation that appears to reach the *coercion* threshold of the nonintervention principle on the basis of official statements or responses from Western like-minded countries.[185]

Framing disinformation as covert election interference. The norm should be framed in such a way that it prohibits concerted Russian *covert* disinformation and influence campaigns aimed at undermining democratic processes while allowing the U.S. and its partners to both allow and sanction *overt* tools to influence elections, for instance by supporting the civil society in the targeted country through formal means, or the informal support of one's own civil society. To this could be added other positive inducements such as trade policy and foreign aid to maintain government and foreign support. Research shows that in contrast to the covert Russian threat described in this case study, most post-Cold War election interference by the United States has been overt, including open support to civil society and democratic processes and aiding

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

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

governments in the hopes of supporting their reelection.[186] Authoritarian regimes, such as Russia, would favor a policy of *total* nonintervention and noninterference in the international affairs of other countries. It would keep Western democracy promotion, support to civil society, aid to opposition parties, public criticism of the Russian regime at bay and offer the Kremlin nearly unopposed internal control.[187] The suggestion above would form a compromise of sorts: overt means of any sort, including 'propaganda' by state media actors such as RT (or from a Russian point of view BBC or CNN), would be considered acceptable, as would however publicly declared funding of civil society organizations (including, for instance, the U.S. National Endowment of Democracy or the Russian Russkiy Mir Foundation) but would disclaim hidden subterfuge including clandestine 'civil society' funding, hacking, or non-transparent strategic communication.

Start with a unilateral ban*.* Robert Knake suggests that the U.S. government takes unilateral action in order to shape global norms in a similar way as the norm against commercial IP theft or political assassinations.[188] He believes U.S. Executive Order 12333 on "United States Intelligence Activities" that bans assassinations would be an expeditious way to internalize and socialize the norm within the U.S. intelligence community and keep the intelligence community from participating in covert election interference. It would not only allow a first-mover advantage in framing the issue but would also combat the perception that liberal democracies such as the U.S. conduct covert influencing activity. The national intelligence community can be persuaded by linking the value of such a norm to the national security interests: "In an era in which election interference tools are not held in a Cold War duopoly but are globally available, creating a strong norm against clandestine interference in democratic processes is in the national security interest of the United States."[189]

Acquire broad support. The entrepreneur should use a coalition or alliance as an organizational platform to socialize the norm with partners and lay the groundwork for opening discussions with Russia on their elections interference and to sanction

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

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

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

189 *Ibid*.

countries that continue to covertly interfere in elections. "As with the agreement with China on economic espionage, the United States and allies would need to agree to abstain from covert election interference even if they are already not doing so in order to allow the Russian government sufficient cover to present any agreement to its citizens as a triumph for Russia."[190] With a broadly supported norm, the United States will be better positioned to create a coalition to punish Russia and other nondemocratic states when their disinformation campaigns covertly interfere in democratic processes.

Second-Order Normative Effects of the Countermeasures

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

Pre-deployment in Russian critical infrastructure establishes a norm of 'mutually assured debilitation'. The unilateral action of the U.S. in pre-deploying within Russia's electrical grids did not occur in a normative vacuum. Clearly, it violated Russia's sovereignty for doing something that is not strictly illegal according to international law. It reaffirms that the U.S. considers sovereignty in cyberspace as more a baseline principle to inform modes of responsible behavior, rather than a set rule. At the same time, it is unlikely that American prepositioning within the Russian power grid constitutes an official renunciation of the agreed UN norm prohibiting cyber operations that damage critical infrastructure.[191] While it may have intruded into the system, U.S. CYBERCOM did not carry out an attack that damaged the critical infrastructure but implicitly threatened such action in order to impose costs sufficient to alter Russian behavior.[192] Even if it does not constitute a direct renunciation of existing norms, it conveys a lack of sincere commitment or double standard that critical infrastructure *may* be included as part of cost imposition against adversaries.

The American public declaration of its willingness to significantly violate the sovereignty of an adversary in peacetime seems to present a novel situation for

190 *Ibid.*

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

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

international law. In an analysis of the U.S. persistent engagement doctrine, Alexander Klimburg describes this second-order effect as follows: "By effectively declaring that the United States considered the pre-deployment of cyber weapons within an adversary's critical infrastructure as permissible (rather than simply being 'caught in the act', as the Russians were), CYBERCOM deviated from the established international legal order that the United States has helped to create." He goes on to say that "It also implicitly accepted a norm of mutual hostage-taking or 'mutually assured debilitation', a huge strategic concession that implies US' acceptance of a level of parity with adversaries where previously it could insist on hegemony."[193] Furthermore, these actions imply that CYBERCOM, and possibly the entire U.S. government, has accepted that 'peacetime' and 'wartime' are artificial distinctions, particularly in the context of the strategic asymmetric domain of cyberspace, reinforcing the Russian and Chinese strategic narratives.

By responding to disinformation with kinetic cyber effects, the U.S. perceives and weaponizes information in the same way as Russia. Klimburg also describes the effects of CYBERCOM's response to the weaponization of information.[194] Although they may have fallen below the threshold of the 'use of force' or 'armed attack' – a distinction not usually made in the United States – they conveyed a public message implying that it is now acceptable to hack what you consider 'fake news' and the weaponization of information. If Russian disinformation is not linked to violations of international law, the U.S. may, through its own countermeasure, undermine existing international law in favor of Russian and Chinese interpretations that argue in favor of negotiating 'good' and 'bad' content. If targeting actors that have a disinformation function, such as the Internet Research Agency, becomes normalized, then similar attacks by Russia and China on conventional media organizations, civil society, and other NGOs may follow. Moscow may consider U.S. support for Russian civil society as 'information and psychological actions aimed at undermining the homeland'.[195] Similarly, Beijing may consider Chinese translations of U.S. newspapers provocative. The new U.S. doctrine and its countermeasures may, therefore, encourage disputes about 'bad content' and lead to the very thing it was intended to alleviate: the weaponization of information.[196]

Media outlets may be labeled as propaganda by political figures. Whilst the actions of the Macron campaign to curtail the well-documented disinformation operations by Russian outlets such as Russia Today were effective, their method of doing so

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

harbors the second-order prospect that other states may employ similar methods against legitimate media outlets. The subsequent efforts of the EU to establish an independent body to track disinformation hints at an attempt to depoliticize the process of designating fake news. However, the normative precedent set by the Macron campaign persists – that media outlets may be labeled illegitimate by political figures or campaigns. Macron's announcements that fake news represents a threat to democracy provides credence for other countries to make the same normative claim, banning or restricting any media they deem as 'fake'. While Western media civil society and NGOs may now be labeled as Western propaganda machines in a similar way, the second-order normative effects are not as profound or further-reaching as the U.S. effects on the weaponization of information.

3.2.4 Key Takeaways

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

In order to avoid risky second-order normative effects, countermeasures to disinformation should refrain from imposing overt kinetic effects. The U.S. doctrine of 'defend forward' and persistent engagement oriented itself around the imposition of costs, directly compromising Russian troll factories and using coercive signaling via pre-deployment in its electrical grids. It thereby conveyed a *public* message implying that it is now acceptable to hack what you consider 'fake news' thereby encouraging disputes about 'bad content'. Ultimately, this may lead to the very thing the doctrine was intended to alleviate: the weaponization of information. Furthermore, by openly communicating about their pre-deployment (rather than being caught in the act) it designated critical infrastructure as a viable vector of coercive signaling - that the range of acceptable cyber targets had expanded to include critical infrastructure, up to the point of threatening 'mutually assured disruption'. Without recognition of the second-

order effects of countermeasures upon the wider cyber and information environment, unintended consequences may undermine the very goals states wish to achieve, and render the broader information security environment more uncertain, hostile and complex. As a comparative case study in countermeasures, the U.S. approach produced a variety of dangerous precedents that will likely inform future calculations of other actor's behavior in cyberspace.

3.3 Case 3: Countering ISIS Propaganda in Conflict Theatres

3.3.1 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.[197] 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*.[198] 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.[199]

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.[200] 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[201] and Telegram[202], and deep web publications such as its flagship publication *Dabiq.*[203]

197 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.

198 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/.

199 Tucker, Patrick, "Why Join ISIS? How Fighters Respond When You Ask Them". The Atlantic, (9 December, 2015).

200 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.

201 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/.

202 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.

203 Gambhir, Harleen, "The Virtual Caliphate: ISIS'S Information Warfare", Institute for the Study of War, (2016), p.20.

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.[204] 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".[205] Its footage was more than one hour long and it included violent depictions ISIS' recent military triumphs.[206] 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.[207]

3.3.2 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 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."[208] From late 2013, the U.S. State Department launched its "Think Again, Turn Away" campaign to counter online Islamist propaganda.[209] Its purpose was to hinder the effects of ISIS propaganda, specifically to dissuade young people from joining the

204 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.

205 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.

206 Fernandez, Alberto, "Here to Stay and Growing: Combating ISIS Propaganda Networks", U.S.-Islamic World Forum Papers, Brookings, (October 2015), pp.8–9.

207 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.

208 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.

209 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.

movement and amplify accounts from ISIS defectors. This campaign was pursued across multiple platforms using multilingual counter-material including YouTube, Facebook and Twitter.[210] 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.[211] 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.[212] 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.[213]

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."[214] 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.[215]

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.[216] 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[217] 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.

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

210 Fernandez, Alberto, "Here to Stay and Growing: Combating ISIS Propaganda Networks", U.S.-Islamic World Forum Papers, Brookings, (October 2015), p.14–16.
211 *Ibid*. p.15.
212 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/.
213 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.;
214 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.
215 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.
216 Throrbberry, 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.
217 Klimburg, Alexander, "The Darkening Web: The War for Cyberspace", Penguin Press, (11 July, 2017).

show that U.S. PSYOPS mainly focuses on broadcast audio messages and the dropping of leaflets.[218]

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.[221] 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.[222] 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.[223] The task force deleted ISIS files, IPs, and accounts.

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."[219] 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".[220]

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.[224] 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.[225] All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.[226]

218 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.

219 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).

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

221 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.

222 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/.

223 *Ibid*.

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

225 *Ibid.*

226 *Ibid.*

Thereafter, the second phase of Operation Glowing Symphony consisted broadly of five operational goals, according to subsequent media reporting:[227]

- 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.[228] 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.[229]

Mandate Cyber Operations: Within the U.S. a distinction is made between Title 50 (offensive operations) and Title 10 authorities (covert intelligence operations).[230] 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.[231] 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.[232]

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."[233] 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.[234]

227 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.
228 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.
229 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.
230 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.
231 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.
232 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.
233 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.
234 *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.[235] The U.K. government employed five lines of action to defeat ISIS, one of which focused on strategic communication.[236] 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."[237] 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.[238] 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.[239] 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.[240] 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.[241] 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.[242] 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.

---

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

236 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/.

237 *Ibid.*

238 *Ibid.*

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

240 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.

241 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.

242 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.

3.3.3 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.

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.[243] 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.[244] 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[245] and cannot harm the former to in pursuit of the latter.[246] The law itself is dubious in applying to cyberspace, notably in suggesting that "media used for military purposes may be lawfully attacked"[247] 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.[248]

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 its

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

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

245 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/.

246 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/..

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

248 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.

effects.[249] This extends to prohibiting "incidental loss or damage to civilian life in excess of concrete or direct military advantage".[250] 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.[251]

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.[252] 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.[253] 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'.[254] 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.[255] In U.S. targeting of foreign servers hosting ISIS' content across six countries, USCYBERCOM took due regard

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

250 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/.

251 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.

252 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.

253 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.

254 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.

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

to comply with IHL principles through forewarning and coordination with the host nations to remove the ISIS presence.[256]

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.[257] 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.[258]

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

256 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.

257 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.

258 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".[259] 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.[260] 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).[261] 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.[262] 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.

---

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

260 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/.

261 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.

262 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.

Second-Order Normative Effects of the Countermeasures

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."[263]

263 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/.

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.[264] 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.[265] 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.[266] 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 of escalation and aggression, as covert offensive cyberspace operations are disclosed in the public domain and consequently underlining a lack of communication.[267] 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

264 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.

265 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.

266 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.

267 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.

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.[268]

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.

3.3.4 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 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.[269] 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,

268 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.
269 See countermeasures to Russian disinformation in the previous case study.

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".[270]

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.[271] 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.[272]

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.

3.4 Case 4: Responding to Chinese Economic Espionage

3.4.1 Incident

This case study focuses on the countermeasures taken primarily by the U.S. and to a lesser extent its Western partners, in response to Chinese cyber-enabled intellectual property theft for commercial gain. The theft that occurred before the U.S. and China reached agreement on a norm in September 2015 prohibiting such actions, as well as the subsequent period. Assessing and measuring espionage trends and impact is rather challenging given its clandestine nature. Yet, many agreed that there was a noticeable

270 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.

271 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.

272 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.

drop in Chinese economic espionage targeting the U.S. in the year following the agreement, albeit with disagreement regarding the underlying reasons for the decrease and explanations as to why and how it resurged from 2017 onwards.

Several Western states and cybersecurity companies – predominantly American – have exposed IP theft campaigns that were carried out by Advanced Persistent Threat (APT) actors affiliated with or coordinated by the Chinese Ministry of State Security (MSS), including APT 10 who is known to target aerospace, telecommunications and government sectors;[273] APT26 who has previously targeted multiple foreign manufacturers of the C919 passenger aircraft;[274] APT3 who stole "files containing commercial business documents" and secret trade data related to GPS, energy and transportation technologies from large US companies".[275] While these operations served economic interests, other cases, such as the Chinese intrusion of Lockheed Martin's networks for F-35 jet technology, served military or national security interests. In other words, they are part of conventional state intelligence operations that not illegal under international law.[276] This entails that this case study will predominantly focus on IP theft for commercial gain, but also illustrates the underlying intentions or motivations for such an operation can and often do overlap, presenting legal or political friction. Thus, the question posed is whether such theft was done as part of an intelligence operation for political-military reasons - and therefore not wholly illegal outside of the scope of international - or an illicit instance of IP theft?

China uses a comprehensive range of economic espionage methods and techniques - encompassing cyber-enabled intrusions to corrupting trusted insiders – in order to improve its competitive edge and its position as an economic and technological leader.[277] Chinese Intellectual Property theft can be contextualized as being one illicit element of a broader state-driven industrial policy (i.e. the industrial policy program *Made in China 2025*) designed to restructure the drivers of modern Chinese economic growth.[278] Aligned with its industrial policy programs, the Chinese predominantly

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

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

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

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

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

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

target high-tech, telecommunications, pharmaceuticals, energy and aviation sectors, and the defense industrial base of South and Southeast Asia, Japan, Taiwan, Hong Kong, South Korea, Europe and the United States.[279] Corporate and technological IP theft provides an innovation injection to alleviate reliance upon foreign technologies and supply chains, and thereby are perceived as being integral for the regime's self-reliance and broader survivability goals, national security and, by extension, protection from foreign interference.[280]

3.4.2 Countermeasures

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

Indictments: The May 2014 indictment of five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization marked an evolution in US' counter-economic espionage strategy - the effectiveness of which has been produced mixed results. The use of indictments continued after the U.S.-China agreement; in November 2017, the Justice Department indicted three Chinese nationals employed by the Chinese cybersecurity firm Boyusec, charging them with hacking into the computer systems of Moody's Analytics, Siemens AG, and Trimble Inc. "for the purpose of commercial advantage and private financial gain."[282] The 2018 indictment of Zhu Hua and Zhang Shilong,[283] two of five Chinese People Liberation Army (PLA) operatives within APT 10, along with the other countermeasures (specifically the bilateral agreement described below) led to a lapse in PLA economic espionage for a limited time. Despite

***Mandate Indictments*:** The legal basis for indictments of the Chinese operatives derives from the Economic Espionage Act (1996) and subsequent amendments through the Defend Trade Secrets Act (2016). Specifically, it outlaws: "economic espionage" (18 U.S. Code § 1831), and "theft of trade secrets" (18 U.S. Code § 1832). Section 1832 requires that the thief is aware that the misappropriation will injure the secret's owner to the benefit of someone else, while section 1831 requires only that the thief intends to benefit a foreign government or one of its instrumentalities. In addition, most of the indictments also include charges for "fraud and related activity in connection with computers" (18 U.S.C. § 1030).[281]

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

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

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

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

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

the typical unenforceability of enacting criminal measures against indicted persons, the use of such legal instruments serves a purpose in lending credence to the U.S. and European ability to more robustly identify specific PLA operatives. This way they can link them to identified APTs and tie them to Chinese economic espionage efforts both as violations of established international law and norms. According to U.S. Attorney General William Barr, the U.S. will continue to issue indictments and prosecutions, which coincide with a statement from FBI Director Christopher Wray saying there are about a thousand investigations involving China's attempted theft of U.S.-based technology.[284]

Sanctions*:* In August 2015, the Obama administration announced it was developing "a package of unprecedented economic sanctions against Chinese companies and individuals" for IP theft.[285] Furthermore, export and import controls and access restrictions were employed in the use of respective technologies by U.S. or Chinese companies.[286] This together with the indictments have increasingly framed bilateral Sino-American relations and acted as momentum for a landmark deal that was reached between then-president Barack Obama and Chinese President Xi Jinping introducing a norm that prohibits IP theft for the benefit of their national economy.[287]

***Mandate Sanctions*:** The existing framework for sanctions within the UN, EU, and U.S. that can be utilized against state and non-state entities is well established and described in detail in Case 1. They encompass a spectrum of measures including individual financial sanctions (asset freezes), trade embargos (flight and shipping bans or export limitations), arms embargoes (prohibition of weapon and dual-use exports), and travel restrictions (visa bans). In the summer of 2015, reports indicated the Obama administration was prepared to use Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," as amended by Executive Order 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities".[288] Furthermore, article 30 of the World Trade Organization's Trade-Related Aspects of Intellectual Property Rights (TRIPS) deals with the protection of undisclosed information.[289] Within the European context, the EU Diplomatic Toolbox can be used to sanction cyber-enabled intellectual property theft.[290]

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

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

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

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

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

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

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

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

Bilateral agreement: From 2013 to 2015 diplomatic (track 1 and 2) exchanges between China and the U.S. took place on various levels, which together with the coercive countermeasures culminated in a Memorandum of Understanding (MOU) introducing an agreement that prohibited cyber-enabled IP theft for the benefit of their respective national economies.[291] In most of the writing about this case, this bilateral agreement is described as introducing a norm; whilst this train of thought is reflected here, it should be noted that a MOU is not a norm *per se* - it is more politically binding. This case is particularly pertinent because the agreement derived from a norm proposal that the U.S. tried and failed to get signed in the 2015 United Nations Group of Governmental Experts. China suffered from not signing this norm within the UN context and got pushed towards agreement on a more politically binding MOU.

The initial bilateral U.S.-China agreement was met with skepticism and mixed reporting, but the consensus is that it resulted in a significant decline in Chinese-attributed intellectual property theft in the following year.[292] This decline was the highest measurable result decline in IP theft as a result of any U.S. countermeasures to date, so its effects should not be underestimated. However, the results were short-lived as Chinese cyber-enabled IP theft returned, albeit in a lower intensity and higher sophistication.[293]

Alternatively, the short period of decline may be attributed to internal Chinese developments. The drop coincided with major structural reforms (i.e. purges) of the Chinese PLA by President Xi that as a result relocated part of the PLA activities, including espionage, to the Ministry of State Security (MSS).[294] After this transition period, the revival of espionage was considered by some to be more sophisticated and

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

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

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

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

targeted, rather than the noisy bulk collection that had previously been conducted.[295] In Europe, the decline has also been linked to a sharp increase in Chinese foreign direct investment and mergers and acquisitions in high-tech and advanced manufacturing industries in 2016.[296]

Ultimately, the resurgent increase in IP theft may be best explained in terms of the deteriorating Sino-American ties after the Trump administration took office, eliminating any incentives that the Chinese had towards adhering to the norm.[297] The resumption of economic espionage led to condemnation from the Five Eyes member countries alongside Japan, Norway, the Netherlands, Germany and Poland.[298] The U.S. has since raised the issue mostly in the context of a larger critique of Beijing's industrial policy and failure to protect IP. It has utilized economic sanctions, including export and import controls and access restrictions to the use of respective technologies by U.S. or Chinese companies.[299] In 2020, the U.S. continued its proactive measures against PLA members citing economic espionage in the Equifax hack aligned with the indictments from the U.S. Justice Department that it had credible attribution means to identify Chinese espionage, which would no longer go undetected.[300] These measures sought to provide freedom for other U.S. departments to leverage cumulative sanctions on Chinese commercial firms, restrictions upon Chinese firms' access to critical supply components, and the imposition of export licensing requirements by the U.S. Department of Commerce.[301] The Trump administration further restricted Chinese investments in particular sectors.[302]

---

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

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

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

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

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

300 *Ibid.*

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

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

In summary, U.S. countermeasures have principally sought to shape Chinese behavior through imposed costs and diplomatic enticement. Acknowledging its comparatively large attack surface area and valuable IP base, the U.S. has preferred coercive countermeasures to compensate for its relatively weak resilience. In contrast, the EU and its member states – having a relatively young cyber sanction mandate and more difficulty coordinating similar coercive measures – have opted to focus on resilience supplemented by less coercive countermeasures. At the same time, Chinese IP theft seems to be a more salient issue to the U.S. than its European counterparts, that, with the exception of Germany, have relatively less commercially attractive IP. Ultimately, the U.S. countermeasures produced the most impactful curbing effect on Chinese cyber-enabled IP theft to date. As Sino-American relations soured, Chinese incentives to adhere to norm diminished and IP theft resurged. Rather than synchronize its countermeasures with its allies, the U.S. decided to impose tariffs against European states, thereby weakening transatlantic relations. The U.S. has stepped towards more aggressive in-band responses in line with its new doctrine on persistent engagement.[303] With this in mind, the following section outlines the normative dimension of these trends and the roles of the respective actors.

3.4.3 The Normative Dimension: What Norms are Promoted?

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

A New Norm Emerges?

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

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

against economic espionage, which specifically focuses on the cyber-enabled theft of intellectual property for economic benefits.

Norm Emergence: Framing and Linking

The norm from the 2015 China-U.S. agreement states that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[304] The main antagonists in the first phase of the norm lifecycle are the *norm entrepreneurs* (primarily the U.S.) that identify the G20 as an *organizational platform* to convince a critical mass of actors to embrace the new norm by *framing* the norm within the context of commercial gains and by *linking* it to economic and national security.

In terms of *framing*, the U.S. limited the norm to cyber-enabled IP theft for *economic benefits*. This excludes other forms of espionage that are conducted for national security benefits. After all, it is not in the U.S. interest to construct a norm that would constrain their intelligence operations within their own national security context. The underlying hope was to get China to accept a distinction between legitimate traditional espionage for political-military ends and illegal espionage for commercial ends.[305]

The U.S. *linked* the norm to the threat it poses to innovation, economic development, and national security, with China identified as the main perpetrator.[306] The norm did not emerge in a vacuum, rather, it has been the result of a longer process. The 2003 U.S. National Strategy to Secure Cyberspace mentioned IP, although it was not a central component of cybersecurity in the 9/11 aftermath. Its importance was raised in the CSIS "Report to the 44th President of the United States on Cybersecurity", where IP protection is not only considered crucial for economic interests but also deemed as important for national security. [307] The Obama administration's "International Strategy for Cyberspace" (2011) included theft of intellectual property as a threat to national security that "threatens national competitiveness and the innovation that drives it".[308]

---

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

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

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

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

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

Subsequent government national security and intelligence assessments strengthen this claim further by significantly expanding the definition of IP or trade secrets, *framing* it as a national security issue, identifying China as the main perpetrator, and using it as a rallying cry for better national cybersecurity. Besides the U.S., countries such as Australia,[309] Germany,[310] the UK,[311] and Canada[312] have all identified intellectual property theft as a cybersecurity issue, though they emphasized its relationship to other kinds of security to various degrees. Likewise, these countries have differed in their willingness to explicitly single out China as the main perpetrator, most likely out of fear of provoking Beijing.

Socialization

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

---

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

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

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

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

The 2015 agreement constituted the pivotal moment in the socialization process.[313] China subsequently agreed to similar bilateral agreements with Australia,[314] Canada,[315] Germany,[316] and the U.K.[317] In November 2015, Brazil, Russia, and other members of the G20 accepted the same norm.[318] Since the threat of IP theft was also socialized within these states – albeit to a much lesser extent than in the U.S. – there was an opportunity to agree on a similar norm with China by bandwagoning on the U.S. tools of influence as China was already socialized towards accepting the norm. The socialization mechanism accelerated when the G20 was used as the organization platform to institutionalize the norm.[319] This in turn led to an ongoing dynamic of imitation and bandwagoning as norm leaders attempt to socialize other actors to become norm followers. For some actors, it may have been in their interest to agree to this norm, while for others maintaining good relations with their respective partners is both a practical and social imperative for maintaining their own status, interest and values, and thus may have adopted the norm not necessarily because of the content but as a form of social camouflage.

Persuasion

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

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

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

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

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

317 Adam Segal, ,"The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age", Public Affairs (23 February, 2016).

318 G20, "G20 Leader's Communiqué Antalya Summit", (16 November, 2015): https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf.

319 *Ibid.*

Coercion

The U.S. used a combination of coercive tools that together created leverage towards the Chinese agreement of a new norm against IP theft for economic purposes. The coercion was largely conducted through naming and shaming, indictments, and the threat of sanctions. Although these tools were first and foremost intended to punish China's bad behavior, they contributed to the subsequent acceptance of the norm by China through signaling that punishment and stigmatization would continue as long as China would continue with IP theft. Other countries did not have to take similar coercive measures as China already adopted the norm with the United States. Australia, for example, remains reluctant to formally attribute and publicly name and shame adversary states engaging in cyber theft for commercial because of the technical uncertainties related to attribution and because of fears of damaging important diplomatic, economic and intelligence relationships.[320]

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

While China may initially appear to adhere to the norm not because of its content but as part of tactical bargains that serve its interests, in response to incentives or coercion, norm internalization or compliance may still become routinized as habits take hold, such that norm-conforming behavior continues even after the incentives. The norm confirmation established by incentives may set in motion organizational and bureaucratic processes that facilitate the internalization of the normative habits by codifying norm-compliance expectations in strategies, rules, procedures, doctrines, rules of engagement, training or other means. In their observations of this case study, some experts have stated that Chinese policymakers believe their shift in tactics, techniques and procedures towards the MSS deploys a higher level of tradecraft that is now equivalent to that of the U.S. National Security Agency. If this is the case, Beijing changed its behavior as a result of the norm and outside pressure, but instead of accepting the distinction that Washington promoted between 'acceptable' and

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

'unacceptable' espionage, they saw it in terms of compartmentalizing its relatively noisy espionage activity to a smaller number and higher level of hacking in line with what it believes the NSA conducts. The Chinese changes in organizational and bureaucratic processes show a change of behavior but not the internalization of the norm the U.S. hoped for when it proposed the 2015 agreement.[321] Finally, China may become *entrapped* by albeit insincere prior rhetorical commitments in ways that push towards norm conformity and sometimes acceptance. The alternative is the danger of appearing hypocritical, which would come with reputational and credibility costs.

Second-Order Normative Effects of the Countermeasures

One of the second-order normative effects of the countermeasures from the first case study also applies to this case, namely that ***politicizing indictments can escalate lawfare***. If we follow the logic that the return to industrial hacking might be a reaction to the increased political and trade tensions between China and the U.S., we can identify two potential negative externalities tied to unilateral U.S. sanctions.

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

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

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

also as a point of Chinese intransigence in the face of an increasingly accepted international norm."[322]

3.4.4 Key Takeaways

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

While the norm and the countermeasures showed promising initial results of Chinese internalization, Chinese behavior now appears to signal an insincere commitment. The so-called return to flouting the established norm may be viewed as the result of souring US-China relations after the departure of the Obama administration and ramping up of the US-China trade war under President Trump. However, it may similarly be viewed as the unilateral actions of China acting in bad faith – agreeing to curb its economic espionage as a pretext to reconstitute its PLA operations for more effective engagement in the future. While China may initially have appeared to adhere to the norm, not because of its content but as part of tactical bargains, that serve their interests in response to incentives or coercion, norm internalization or compliance may still become routinized as habits take hold. Furthermore, the norm provides an important yardstick as China becomes *entrapped* by the reciprocal consequences of insincere prior rhetorical commitments in ways that push towards norm conformity and potential acceptance. The alternative is the danger of appearing hypocritical, which would come with reputational and credibility costs.

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

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

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

3.5 Case 5: Upholding Freedom of Navigation in the South China Sea

3.5.1 Incident

This case study addresses the normative dimensions of China's actions and claims of exclusive territorial authority over contested areas of the South China Sea. They are challenging the well-established norms of innocent passage and freedom of navigation that have their propriety in the UN Convention on the Law of the Sea (UNCLOS) – the most comprehensive and widely ratified framework maritime security framework. While China ratified the convention, which should increase the likelihood of norm internalization, it is now walking back on its commitment stating that in retrospect it was not knowledgeable and well-prepared enough to ratify it at the time. It is important to stress that the U.S. has not ratified the UNCLOS, but is still bound to its components that have reached the status of customary international law. The emergent norms introduced by China, and the reciprocal norms introduced or reasserted by actors like the U.S. in their countermeasures, are subsequently addressed in line with their first and second-order implications.

In order to strengthen its claims to the South China Sea, China relies on a twin pillar strategy: its purported *historical right* to its territorial claims and its mandate under the purported *nine-dash line*.[323] China has maintained a political strategy of cultivated

323 While the 9-dash line dates back to the 1940s, it took until May 2009 before it received international attention when China used it in its objection to the Malaysian-Vietnamese joint submission and Vietnamese individual submission to the Commission on the Limits of the Continental Shelf. The use of the nine-dash line has been inconsistent at best – it went from eleven to nine, and then back to ten, dashes to include Taiwan. Benatar, Marco; Franckx, Erik. "Dots and Lines in the South China Sea: Insights From the Law of Map Evidence", Asian Journal of International Law 2, no. 1, (January 2012), pp. 89-118: https://www.cambridge.org/core/journals/asian-journal-of-international-law/article/dots-and-lines-in-the-south-china-sea-insights-from-the-law-of-map-evidence/328F9E4996170DF296D42A287B1E479A. Berkovsky, Axel, "US Freedom of Navigation Operations (FONOPs) in the South China Sea—Able to Keep Chinese Territorial Expansionism in Check?", in "US Foreign Policy in a Challenging World: Building Order on Shifting Foundations", ed. Marco Clementi, Matteo Dian, and Barbara Pisciotta (Cham: Springer, 2018), pp.343-344.

ambiguity, avoiding detailed justification for the legitimacy its claims whilst touting alleged historic rights to the disputed territories.[324] China regularly employs vague terminology which conflates the distinction between maritime claims and territorial claims, especially in its construction of artificial islands as a means to establish effective control over the islands and its adjacent maritime zones. The "Nine-Dash Line" demarcates the current contested area spanning much of the South China Sea, from Hainan Island down to the top of Indonesia.[325] Beijing has provided no specific coordinates or clarifying details to the document, instead opting to leverage its cultivated ambiguity as a bargaining chip in its political strategy.[326] Both claims are loosely defined and have been regularly contested both within international law and by the other claimant states.[327]

In practice, Beijing has employed a spectrum of measures ranging from paramilitary and law enforcement agencies, assertive fishing activity, and the construction of artificial islands and military bases to enforce Chinese law, expand its presence, and bolster what it perceives as its rightful claim. From 2009 onward, it has built-up of its military facilities within the contested area, in tandem with assertive patrols and exercises. According to the 2019 U.S. Department of Defense Report, many occupied islands – notably the Spratly Islands - have been fitted with anti-air and anti-sea capabilities, in violation of a 2015 pledge by Xi Jinping that "China does not intend to pursue militarization" of the islands.[328] From 2014, it aggressively pursued land reclamation efforts, producing thousands of acres of new landmass for civilian and military purposes.[329]

---

324 Since its first official reference to historical rights in 1998, China has reiterated its exclusive maritime rights without defining their legal basis, stating its sovereignty over the disputed islands as a matter of fact. The islands include the Paracel and Spratly islands, as well as a collection of reefs and shoals, such as Mischief Reef and the Scarborough Shoal. The historic appeal to territorial rights over the concerned islands refers to the times in which the islands were under the integral rule of Imperial China, with recent studies indicating that the claim as such originated at the beginning of the 20th century. See Hayton, Bill, "The Modern Origins of China's South China Sea Claims: Maps, Misunderstandings, and the Maritime Geobody", Modern China (4 May, 2018): https://journals.sagepub.com/doi/abs/10.1177/0097700418771678?journalCode=mcxa.

325 Beech, Hannah, "Just Where Exactly Did China Get the South China Sea Nine-Dash Line From?", TIME (19 July, 2016): https://time.com/4412191/nine-dash-line-9-south-china-sea/.

326 Wong Chun Han, "Nine-Dash Line's Ambiguity a Good Thing, Argues Chinese Military Academic", Wall Street Journal (5 June, 2016): https://blogs.wsj.com/chinarealtime/2016/06/05/nine-dash-lines-ambiguity-a-good-thing-argues-chinese-military-academic/.

327 United States Office of Ocean and Polar Affairs, "Limits in the Sea", U.S. State Department (5 December,2014): https://news.usni.org/2014/12/09/document-u-s-state-department-report-chinas-claims-south-china-sea; Regencia, Ted, "Malaysia FM: China's 'Nine-Dash Line" Claim 'Ridiculous", Aljazeera (21 December, 2019): https://www.aljazeera.com/news/2019/12/malaysian-top-envoy-china-dash-line-claim-ridiculous-191221034730108.html.

328 United States Office of the Secretary of Defense, "Annual Report to Congress – Military and Security Developments Involving the People's Republic of China 2019", Department of Defense, (2 May, 2019): https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

329 Grossman, Derek, "Military Build-Up in the South China Sea", in The South China Sea: From a Regional Maritime Dispute to Geo-Strategic Competition", ed. Leszek Buszynski and Do Thanh Hai (2020).

China has significantly upgraded its overall naval capabilities across different services, which have exercised maritime control in the area.[330] That control has been exercised partly by military coast guards but more prominently by patrolling paramilitary law enforcement agencies.[331] China has also sought to tighten its hold over the region in symbolic ways. The nine-dash line is portrayed on Chinese passports and in April 2020, it created two new administrative districts covering the Spratly and Paracel islands under the notional Sansha city; it has also named 80 geographical features in the South China Sea. By taking these efforts, it seeks to reinforce its legally inchoate claims as a matter of undisputed fact rather than a disputed legal contest.[332]

The underlying reasons for China's maritime and territorial claims in the South China Sea are manifold and partly overlap. Control over the area offers strategic and security gains through an expanded Southern sphere of control that secures its supply lines, strengthens its military position vis-à-vis Taiwan, controls subsea natural resources, such as gas and oil fields, while pushing the U.S. (and other Western) navy out. Beijing seeks to exercise control and assert sovereignty in the region through a careful balance between "safeguarding rights and maintaining stability".[333] The term coined to describe these actions – known as 'talk and take' – denotes China's dual-use of expansion and entrenchment, coupled with the proclaimed facade that it is willing to engage in peaceful talks with other litigant states to resolve their issues.[334] This ostensible accommodating diplomatic outlook rarely materializes beyond rhetoric and is generally viewed as a means by which China can deescalate and prolong international discussions whilst it entrenches and normalizes its territorial presence and pursues its ambition of the nine-dash line.[335] The following section will outline the countermeasures employed by the U.S. and their regional allies in response to this behavior, and their role in bolstering UNCLOS.

3.5.2 Countermeasures

The countermeasures employed against Chinese conduct have ranged from legal (arbitration), military (Freedom of Navigation Operations), to diplomacy.

---

330 Erickson, Andrew S.; Hickey, Joshua; Holst, Henry, "Surging Second Sea Force: China's Maritime Law Enforcement Forces, Capabilities, and Future in the Gray Zone and Beyond", Naval War College Review 72, no. 2 (2019), pp. 11–34.

331 Morris, Lyle, "Gray Zone Challenges in the East and South China Sea", Maritime Issues, (7 January 2019): http://www.maritimeissues.com/politics/gray-zone-tactics-and-their-challenge-to-maritime-security-in-the-east-and-south-china-sea.html.

332 Economist, "China's Next Move in the South China Sea", (18 June, 2020): https://www.economist.com/china/2020/06/17/chinas-next-move-in-the-south-china-sea.

333 Zhang, Cheng, "China's Long March at Sea: Explaining Beijing's South China Sea Strategy, 2009–2016", The Pacific Review, (2020): https://doi.org/10.1080/09512748.2019.1587497.

334 Beukel, Erik, "China and the South China Sea: Two Faces of Power in the Rising China's Neighborhood Policy", Danish Institute for International Studies, Copenhagen (2010): https://www.econstor.eu/handle/10419/44627.

335 Corr, Andrew, "China's Take-and-Talk in the South China Sea", Forbes (29 March, 2017): https://www.forbes.com/sites/anderscorr/2017/03/29/chinas-take-and-talk-strategy-in-the-south-china-sea/#69887aa33216.

Arbitration: The most well-known legal countermeasure was the case brought against China by the Philippines, triggering a legal process that lasted from 2013 to 2016.[336] The Tribunal in The Hague ultimately ruled in favor of the Philippines' claim that China violated its sovereign rights, with the rule being appraised as "a major victory for [the] Philippines".[337] Nevertheless, this ruling had little impact on the realities on the ground, principally due to a lack of political commitment from Manilla brought upon by a change in leadership.[338] Specifically, the tribunal ruled that China's claims of 'historic rights' encompassed by the nine-dash line are superseded by its maritime rights and obligations under the Law of the Sea Convention.[339]

Chinese officials claimed this ruling was "null and void", and refused to abide by it.[340] It has since reinforced its presence along its artificial islands with increased anti-air and anti-sea capabilities, and voiced tentative claims to establishing an air defense identification zone (ADIZ) over the Pratas, Paracel and Spratly island groups.[341] Legal countermeasures, therefore, have not produced a real resolution to the dispute, nor have they prevented China from pursuing its objectives in the South China Sea.

FONOPs: As the principal enactor of countermeasures, the U.S. has pursued an approach rooted in the objectives of its domestic and foreign security, economic prosperity, and the upholding of international law.[342] Its attempts to uphold the principle of Freedom of Navigation have primarily been conducted through the framework of **freedom of navigation operations (FONOPs)**.[343] In recent years, the U.S. has repeatedly and ever-more frequently instructed its warships to sail within the 12 nautical miles distance from China's claimed territories, signaling their nonacceptance of Chinese claims of sovereignty over the islands.[344] The U.S. Navy frames these FONOPs as challenging excessive Chinese territorial claims - their notional intent of

336 Permanent Court of Arbitration, "Press Release – The South China Sea Arbitration", The Hague (12 July, 2016): https://www.pcacases.com/web/sendAttach/1503; New York Times, "Hague Announces Decision on South China Sea", (12 July, 2016): https://www.nytimes.com/interactive/2016/07/12/world/asia/hague-south-china-sea.html.

337 Kuok, Lynn, "How China's Actions in the South China Sea Undermine the Rule of Law", Brookings (November 2019), p.2: https://www.brookings.edu/research/how-chinas-actions-in-the-south-china-sea-undermine-the-rule-of-law/

338 *Ibid.*

339 Perlez, Jane, "Tribunal Rejects Beijing's Claims in South China Sea", New York Times, (12 July, 2016): https://www.nytimes.com/2016/07/13/world/asia/south-china-sea-hague-ruling-philippines.html.

340 Tiezzi, Shannon, "China: Tribunal Ruling 'Null and Void', Will Not Affect South China Sea Claims", The Diplomat (12 July, 2016): https://thediplomat.com/2016/07/china-tribunal-ruling-null-and-void-will-not-affect-south-china-sea-claims/.

341 U.S.-China Economic and Security Review Commission, "ADIZ Update: Enforcement in the East China Sea, Prospects for the South China Sea, and Implications for the United States", (2 March, 2016): https://www.uscc.gov/research/adiz-update-enforcement-east-china-sea-prospects-south-china-sea-and-implications-united.

342 Green et al., "Countering Coercion in Maritime Asia", Asia Maritime Transparency Initiative, (9 May, 2017): https://amti.csis.org/countering-coercion-hub/.

343 McDevitt, Michael, "The South China Sea: Assessing U.S. Policy and Options for the Future", CNA (November, 2014), p.6: https://theasiadialogue.com/wp-content/uploads/2017/08/IOP-2014-U-009109.pdf.

344 Larter, David, "In Challenging China's Claims in the South China Sea, the US Navy is Getting More Assertive", DefenseNews (February 5, 2020): https://www.defensenews.com/naval/2020/02/05/in-challenging-chinas-claims-in-the-south-china-sea-the-us-navy-is-getting-more-assertive/.

missions being to reassert the internationally established UNCLOS, especially the right of innocent passage. In this respect, U.S.' operations challenge the notion that innocent passage through claimed territorial waters requires previous notification or approval, of which Beijing regularly contests as a prerequisite for FONOPs.[345]

Whilst earlier FONOPs were sporadic and only numbered few per year, they have become more frequent, with the record achieved in 2019 in which nine FONOPs were conducted altogether.[352] So far, in 2020 the U.S. conducted one operation in January near the Spratly islands (by the combat littoral ship *Montgomery*)[353] and two operations in April both near the Spratly and Paracel islands (by the *USS Bunker Hill* and the *USS Barry*, respectively).[354] When conducting operations, the U.S. does not ask for permission to enter contested zones.[355] In recent years, similar operations have also been conducted by the U.K.[356] and France[357], though these countries have

Mandate UNCLOS - Right of Innocent Passage: Article 17 of the UNCLOS stipulates "ships of all States, whether coastal or land-locked, enjoy the right of innocent passage through the territorial sea." Article 19 defines innocent passage as any action "not prejudicial to the peace, good order or security of the coastal State." Actions considered prejudicial encompass the "threat or use of force", "the launching, landing or taking on board of any aircraft", "collecting information", "carrying out research or survey activities"[346] Some states, including China, have claimed the right of prior authorization, or at least prior notification, of vessels transiting under the right of innocent passage.[347] This demand is contested by Article 24 (1) UNCLOS, which forbids coastal states from imposing "requirements on foreign ships which have the practical effect of denying or impairing the right of innocent passage".[348]

Mandate FONOPS: The legal justification for the conduct of FONOPs relies on "freedom of navigation", one of the most salient and well-established maritime rules that are a part and parcel of international customary law.[349] The U.S. doctrinal basis for FONOPs was established by the joint effort of the U.S. Department of Defense and Department of State in 1979 when it conveyed a broad range of measures, including diplomatic consultations and military operations.[350] Since its inception, the U.S. has relied on the international mandate and its national doctrine to conduct FONOPS in various regions.[351]

345 *Ibid.*
346 United Nations, "Article 19 – Innocent Passage", Part II Territorial Sea and Contiguous Zone, (2020): https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm.
347 Starting, Rebecca, "Defending the Maritime Rules-Based Order: Regional Responses to the South China Sea Disputes", Policy Studies (80), East-West Center, (2020): https://www.eastwestcenter.org/system/tdf/private/ewc_policy_studies_80_-_defending_the_maritime_rules-based_order_-regional_responses_to_the_south_china_sea_disputes.pdf?file=1&type=node&id=37485.
348 United Nations, "Article 24 – Innocent Passage", Part II Territorial Sea and Contiguous Zone, (2020): https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm; Hakapää, Kari, "Innocent Passage", Oxford Public International Law, (2013): https://www.ilsa.org/Jessup/Jessup18/Second%20Batch/OPIL_Innocent_Passage.pdf.
349 Wolfrum, Rudiger, "International Tribunal for the Law of the Sea", Freedom of Navigation (2010): https://www.itlos.org/fileadmin/itlos/documents/statements_of_president/wolfrum/freedom_navigation_080108_eng.pdf.
350 Mandsager, Dennis, "The U.S. Freedom of Navigation Program: Policy, Procedure, and Future", International Law Studies (72), (1998): https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1465&context=ils.
351 United States Office of the Under Secretary of Defense, "DoD Annual Freedom of Navigation (FON) Reports", OUSDP Office (2020): https://policy.defense.gov/OUSDP-Offices/FON/.
352 Power, Josh, "US Freedom of Navigation Patrols in South China Sea Hit Record High in 2019", South China Morning Post (5 February, 2020): https://www.scmp.com/week-asia/politics/article/3048967/us-freedom-navigation-patrols-south-china-sea-hit-record-high.
353 Ziezulewicz, Geoff; Snow, Shawn, "Navy Conducts Year's First FONOP in South China Sea", Navy Times (28 January, 2020): https://www.navytimes.com/news/your-navy/2020/01/28/navy-conducts-years-first-fonop-in-south-china-sea/.
354 Maritime Executive, "U.S. Navy Conducts Two South China Sea FONOPS in Two Days", (30 June, 2020): https://maritime-executive.com/article/u-s-navy-conducts-two-south-china-sea-fonops-in-two-days.
355 Paul Michael, "The United States, China and the Freedom of the Seas: Washington's FONOPs Conflict with Beijing" Stiftung Wissenschaft und Politik, (2016), p. 2: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-46539-4.
356 Hemmings, John, "Charting Britain's Moves in the South China Sea", RUSI (6 February, 2019): https://rusi.org/commentary/charting-britain%E2%80%99s-moves-south-china-sea.
357 Navy Recognition, "French Navy Frigate Conducts FONOP in South China Sea", (23 March, 2018): https://www.navyrecognition.com/index.php/news/defence-news/2018/march-2018-navy-naval-defense-news/6081-french-navy-frigate-conducts-fonop-in-south-china-sea.html.

been less explicit about the purpose of the operations and labeled them 'patrolling actions' instead. Australia has conducted flights in the area for the same purpose.[358] Japan, India and the Philippines have recently joined the U.S. resulting in multinational FONOPs that send a powerful symbolic signal to China.[359] This is particularly relevant as Beijing believes FONOPs by extra-regional powers destabilize peace and order in the South China Sea. However, as some observers have pointed out, despite the increase in frequency, these countermeasures have failed to stop Chinese efforts to assert control in the area. Beijing displays typical great power behavior to this end: it aims to minimize all possible threats close to its borders and will simply not budge to foreign pressure.

Diplomatic countermeasures have included a wide range of multilateral and bilateral initiatives. These include the U.S.-Japan-Australia-India quadrilateral dialogue and joint efforts to a joint Indo-Pacific strategic space that gas garnered support and interwoven the geopolitics of both bodies of water, including the South China Sea. Amongst other things, the strategy emphasizes respect for international rules, including freedom of navigation and overflight: "The US has offered support for these principles on various fronts, including expanding U.S. Freedom of Navigation operations in contested areas of the South China Sea, increasing maritime capacity building support for Southeast Asian and Pacific Island nations, working alongside G-20 leaders to promote new Principles for Quality Infrastructure Investment, and announcing a new $400 million Indo-Pacific Transparency Initiative."[360] The EU – with the longest maritime border in the world – has also become more involved as it has the ambition to become a net maritime security provider.

Chinese diplomatic engagement is set at barring extra-regional actors from meddling, unless deemed constructive by China, meaning that those actors would have to support Chinese claims or shelve their disputes with Beijing. China's approach is more focused on gaining wins through bilateral engagements than sincere multilateral cooperation within ASEAN. The most notable example of the latter is the effort to reach a Code of Conduct within the ASEAN framework, which can be traced back to the 1990s, with milestones reached being the Declaration on the Conduct of Parties in the South China Sea (2002), and in 2016 when the two sides formally and jointly worked toward the adoption of a Code of Conduct rooted in mutual consensus.[361] Nonetheless, diplomatic engagement with China seems to have made little impact so far – a reflection of the

358 BBC, "Australia Conducting 'Freedom of Navigation' Flights in South China Sea", (15 December, 2015): https://www.bbc.com/news/world-australia-35099445.

359 DeAeth, Duncan, "US, Japan, India, Philippines Conduct Joint Naval Patrol Through South China Sea", Taiwan News (9 May, 2019): https://www.taiwannews.com.tw/en/news/3698009.

360 Ford, Lindsey, "The Trump Administration and the 'Free and Open Indo-Pacific'", Brookings Institute (May, 2020): https://www.brookings.edu/wp-content/uploads/2020/05/fp_20200505_free_open_indo_pacific.pdf.

361 ASEAN, "Joint Statement of the Foreign Ministers of ASEAN Member States and China on the Full and Effective Implementation of the Declaration on the Conduct of Parties in the South China Sea", (25 July, 2016): https://asean.org/storage/2016/07/Joint-Statement-on-the-full-and-effective-implementation-of-the-DOC-FINAL.pdf, p.1.

'talk and take' stigma they have garnered.[362] China continuously stresses its peaceful intentions and willingness to cooperate on the management of maritime resources, whilst simultaneously perpetuating dialogue as a smokescreen for consolidating its claims.[363] Beijing has reportedly proposed that the code of conduct requires unanimous approval by all ASEAN members – who are notoriously split by and over China - for military exercises involving countries outside of China or ASEAN in the South China Sea, a move likely intended to impede US-allied FONOPS.[364]

China's policy of 'talk and take', in which it reassures regional neighbors of its peaceful intentions and willingness to jointly manage maritime resources without showing any meaningful commitment, has been largely successful.[365] The more time passes, the more economic and military power China gains, and the more able it will be to outlive its competitors and reach its long-term objectives in the South China Sea simply because other stakeholders cannot or will not hold their ground anymore. Their success is due to a number of factors, including: power asymmetries with and between its neighbors, economic entanglement propelled by the Belt and Road Initiative, the absence of a regional security architecture, and, most recently, hardening positions by the major players.[366] In these circumstances, the ambiguity surrounding China's maritime claims – especially concerning the lack of clarity on the nine-dash line – contributes to the perpetuation of discussions. As long as Beijing does not clarify its position, joint cooperation would seem unlikely. Military countermeasures from China's neighbors are limited to the buildup of their national defenses, improvement of their anti-access and area denial capabilities, the expansion of their coast guard's presence, and the pursuit of their own land reclamation efforts.[367] All efforts are, however, dwarfed by the parallel Chinese developments.

In summary, the countermeasures employed in curtailing Chinese behavior have thus far failed to produce tangible results and deter China's expansive presence over the region. The next section situates these realities within the normative context, juxtaposing the conflict between existing and emerging norms presented by the opposing sides.

---

362 Guzman, Luchi de, "ASEAN Targets Completion of Code of Conduct Within Three Years", CNN (4 November, 2019): https://www.cnnphilippines.com/news/2019/11/41/asean-china-code-of-conduct-south-china-sea.html.

363 Reuters, "Xi Jinping Says China Wants South China Sea Issues Resolved Peacefully", The Guardian (7 November, 2015): https://www.theguardian.com/world/2015/nov/07/xi-jinping-says-china-wants-south-china-sea-issue-resolved-peacefully; Fravel, Taylor, "China's Strategy in the South China Sea", Contemporary Southeast Asia 33(3), (2011) pp. 292-319: https://taylorfravel.com/documents/research/fravel.2011.CSA.china.strategy.scs.pdf.

364 United States Office of the Secretary of Defense: "Annual Report to Congress – Military and Security Developments Involving the People's Republic of China 2019", Department of Defense, (2 May, 2019) p.86: https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

365 Corr, Andrew, "China's Take-and-Talk in the South China Sea", Forbes (29 March, 2017): https://www.forbes.com/sites/anderscorr/2017/03/29/chinas-take-and-talk-strategy-in-the-south-china-sea/#69887aa33216.

366 Storey, Ian, "China Pushes on the South China Sea, ASEAN Unity Collapses", China Brief 12, no. 15 (2012): p.59

367 Most notably Vietnam, and to a lesser extent Indonesia, Malaysia and the Philippines; see Kuok, Lynn, "How China's Actions in the South China Sea Undermine the Rule of Law", Brookings (November 2019): https://www.brookings.edu/research/how-chinas-actions-in-the-south-china-sea-undermine-the-rule-of-law/. Grossman, Derek, "Military Build-Up in the South China Sea', in The South China Sea: From a Regional Maritime Dispute to Geo-Strategic Competition", ed. Leszek Buszynski and Do Thanh Hai, Routledge, (2020), pp. 7-8.

3.5.3 The Normative Dimension: What Norms are Promoted?

This section examines norm emergence on the part of China's role as a norm entrepreneur, and how it conflicts with existing norms and rules, most notably the UNCLOS, as well as explain how tools of influence are used to bolster both norm developments. As a normative incidence, Chinese actions in the pursuit of its claims erode the United Nations Convention on the Law of the Sea (UNCLOS).[368] Crucially, Chinese actions seek to revise the "rule of innocent passage" by barring foreign navies access to its territorial sea[369] and Exclusive Economic Zones (EEZ)[370] without prior consent. China reserves exceptions of this principle to its own actions while observers believe it does not abide by this rule itself.[371] Moreover, the case shows that the seemingly internalized norms of innocent passage that are enshrined in customary international law do not remain fixed or unchallenged. As the international context changes, the norm changes with it.

While FONOPs are unlikely to be sufficient by themselves, the U.S. and its allies are arguably establishing it as an acceptable enforcement mechanism tool for freedom of navigation and of the right of innocent passage – both cornerstone norms of Hugo Grotius' *mare liberum* and enshrined in the UNCLOS and customary international law.[372] These norms, and by extension UNCLOS, are not only essential to upholding maritime security in the South China Sea, its Sea Lines of Communication (SLOCs), but also for protecting the existing balance of coastal state rights and international rights of freedom of navigation from Chinese encroachments.[373]

368 Xue, Guifang, "China and the Law of the Sea: An Update", International Law Studies 84, (8 January, 2008), pp. 97-98: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1143&context=ils.

369 The Territorial Sea is described in Part II of the UNCLOS. It extends the territorial sovereignty of a coastal states up to 12 nautical miles from the baseline and includes the air space as well. Ships of all states still enjoy the right of innocent passage through the territorial sea. United Nations "Part II Territorial Sea and Contiguous Zone." Law of the Sea, (2020): https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm.

370 The Exclusive Economic Zone (EEZ) is described in Part V of the UNCLOS. It extends up to 200 nautical miles from the baseline from which the territorial sea is measured and offers the coastal states with *sovereign rights* "for the purpose of exploring and exploiting, conserving and managing the natural resources". The state has jurisdiction over the establishment and use of artificial islands, installations and structures; marine scientific research; and the protection and preservation of the marine environment. United Nations, "Part V of the UNCLOS" Law of the Sea, (2020): https://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm.

371 Michael, Paul, "The United States, China and the Freedom of the Seas: Washington's FONOPs Conflict with Beijing", Stiftung Wissenschaft und Politik, (2016), p.3: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-46539-4; Fletcher School, "Freedom of Navigation", Law of the Sea – A Policy Primer, TUFTS (24 May, 2016): https://sites.tufts.edu/lawofthesea/#:~:text=The%20law%20of%20the%20sea%2C%20as%20embodied%20in%20the%20Law,international%20framework%20for%20the%20conservation%2C.

372 *Ibid*.; United Nations, "United Nations Convention on the Law of the Sea – Agreement Relating to the Implementation of Part XI of the Convention", UN Law of the Sea: https://www.un.org/Depts/los/convention_agreements/texts/unclos/closindx.htm.

373 Holmes, James, "Are Freedom of Navigation Operations in East Asia Enough?", The National Interest (23 February, 2019): https://nationalinterest.org/feature/are-freedom-navigation-operations-east-asia-enough-45257; Ben, Cardin, "The South China Sea is the Reason the United States Must Ratify UNCLOS", Foreign Policy (13 July, 2016): https://foreignpolicy.com/2016/07/13/the-south-china-sea-is-the-reason-the-united-states-must-ratify-unclos/.

A New Norm Emerges?

China has propagated a new norm of behavior by challenging the UNCLOS principle of Freedom of Navigation to what is described by some observers as dovetailing with its interest to localize law and push for specific regional maritime governance, due to what Beijing describes as a different or even unique historical context.[374] First, it is challenging UNCLOS norms that determine how states lay claim to maritime zones, such as the Exclusive Economic Zones (EEZs), by reverting to historical rights, the nine-dash line, and the construction of artificial islands. By claiming exclusive authority over the South China Sea in ways not supported by international law (UNCLOS), China challenges the only global maritime security framework, and campaigns for a revisionist norm.[375] Second, it is challenging the right of innocent passage of foreign navies by barring them or by requiring previous authorization.[376] This emerging norm is in conflict with the pre-existing norm internalized by the majority of states around the world which many, most explicitly the U.S., seek to enforce.[377]

These normative revisions seek to challenge the existing balance of coastal state rights and international rights of freedom of navigation through China's use of various tools of influence.[378] This not only affects the other regional actors in the South China Sea, but risks potentially destabilizing first and second order effects for countries with Sea Lines of Communication (SLOCS) or vessels transiting through the South China Sea.[379] The following section outlines how the two sides have used a combination of tools of influence – socialization, persuasion and coercion - to propagate and cultivate their respective norms.

Socialization

China has attempted to socialize other countries into accepting the norm supporting its claims to the area. One form of socialization is the periodic uptick of supportive publications *linking* the issue in terms of Chinese *historic rights* to the contested area.[380] The mainstay publication platform for this effort has been Chinese academic

374 Franki, Julie, "Seize the Sea: the Territorial Conflict Between the United States and China Over Military Operations in the South China", Emory (31), pp. 1026-1027: https://law.emory.edu/eilr/_documents/volumes/31/recent%20developments/franki.pdf,.

375 Permanent Court of Arbitration, "In the Matter of the South China Sea Arbitration", (12 July, 2016): https://pcacases.com/web/sendAttach/2086.

376 Thu, Huong Le, "China's Incursion into Vietnam's EEZ and Lessons From the Past", Asia Maritime Transparency Initiative (8 August, 2019): https://amti.csis.org/chinas-incursion-into-vietnams-eez-and-lessons-from-the-past/.

377 Although it is necessary to point out that there is a substantial number of states that, though independently of each other, agree with China on posing restrictions on navigation, both in formal expressions and in terms of behavior. See the table in Pham, Trand; Truong-Minh Vu, "From Clash of Vision to Power Struggle: The US, China, and Freedom of Navigation", E-International Relations (31 October, 2014): https://www.e-ir.info/2014/10/31/from-clash-of-vision-to-power-struggle-the-us-china-and-freedom-of-navigation/.

378 Kuok, Lynn: "How China's Actions in the South China Sea Undermine the Rule of Law", Brookings (November 2019): https://www.brookings.edu/wp-content/uploads/2019/11/FP_20191118_china_scs_law_kuok.pdf.

379 Glaser, Bonnie, "Conflict in the South China Sea", Council on Foreign Relations (2015): https://www.cfr.org/report/conflict-south-china-sea.

380 For a complex overview of this literature, see Zheng Wang, Chinese Discourse on the "Nine-Dashed Line: Rights, Interests, and Nationalism", Asian Survey , Vol. 55, No. 3 (May/June 2015), pp. 502-524.

journals, which contain a plethora of articles advocating the Chinese perspective on the issue.[381] Moreover, these publications tend to link Chinese claims to the irrelevance of international law, which supposedly cannot overwrite historic claims, and advocate Chinese behavior by pointing at "China's responsible attitude" as the salient reason for stability in the region.[382] Others have questioned the 2016 tribunal ruling on the basis of its supposedly incorrect interpretation of international law and inconsistent terminology.[383] These publications have been accompanied by similar *framing* devices explicitly spelled out by Chinese officials.[384] China has compounded its historical argument through analogy, drawing parallels to the perceived 'century of humiliation' of 1839-1949 in which China suffered intervention by Western, Russian and Japanese powers.[385] This cultural touchstone is regularly leveraged by the Chinese Communist Party to mobilize support domestically and abroad amongst anti-colonial audiences, portraying its actions not as expansionist but as a justified restoration of China's sovereign rights and geopolitical status.[386]

Beijing has also established official names for the recently created pieces of land, framing their identity and signaling their permanent legal status under Chinese sovereignty.[387] Furthermore, Chinese passports depict the contested territories and the nine-dash line forming part of China, a move that has provoked angry reactions from the Philippines and Vietnam.[388] Moreover, it has established two new city districts on Woody island and more broadly over 280 island shoals, reefs and features, developing their administrative control over the territories.[389] These newly created districts entrench and normalize China's perceived sovereignty, and the influx of Chinese tourism to the area brings increased ship

381 YEE, Sienho, "Chinese Journal of International Law", (2020): https://academic.oup.com/chinesejil.

382 Hao, Su, "China's Positions and Interests in the South China Sea: A Rational Choices in its Cooperative Policies", CSIS (12 September, 2011): https://www.csis.org/analysis/china%E2%80%99s-positions-and-interests-south-china-sea-rational-choices-its-cooperative-policies.

383 Gau, Michael Sheng-ti. "The Interpretation of Article 121(3) of UNCLOS by the Tribunal for the South China Sea Arbitration: A Critique." Ocean Development & International Law 50, no. 1 (January 2, 2019), pp. 49–69: https://doi.org/10.1080/00908320.2018.1511083.

384 Vincenti, Daniela, "South China Sea Arbitration: Illegal, Illegitimate and Invalid", EURACTIV (12 July, 2016): https://www.euractiv.com/section/global-europe/opinion/south-china-sea-arbitration-illegal-illegitimate-and-invalid/.

385 Raunig, Colin: "A Sense of Sovereignty: How China's 'Century of Humiliation' Affects U.S. Policy in the South China Sea", Naval History and Heritage Command, (2017): https://www.history.navy.mil/content/history/nhhc/get-involved/essay-contest/2017-winners/additional-essay-contest-submissions/a-sense-of-sovereignty---how-chinas-century-of-humiliation-affec1.html; Heller, Christian: "South China Sea: China Breaks From a Century of Humiliation", RealClearDefense, (4 February, 2019): https://www.realcleardefense.com/articles/2019/02/04/south_china_sea_china_breaks_from_a_century_of_humiliation_114158.html.

386 Callahan, William, "National Insecurities: Humiliation, Salvation, and Chinese Nationalism", Alternatives: Global, Legal, Political 29 (2), (May 2004), pp. 199-218: https://www.jstor.org/stable/40645112?seq=1

387 Lei, Zhao, "Ministries Release Official Names for South China Sea Entities", China Daily (20 April, 2020): https://www.chinadaily.com.cn/a/202004/20/WS5e9d3404a3105d50a3d176e8.html; Odom, Jonathan, 'Protecting the Rules-Based Order at the International Tribunal for the Law of Sea', Lawfare (8 May, 2020): https://www.lawfareblog.com/protecting-rules-based-order-international-tribunal-law-sea.

388 Mogato, Manuel, "China Angers Neighbors With Sea Claims on New Passports", Reuters (22 November, 2012): https://www.reuters.com/article/us-china-southchinasea/china-angers-neighbors-with-sea-claims-on-new-passports-idUSBRE8AL09Q20121122.

389 Yamaguchi, Shinji, "Creating Facts on the Sea: China's Plan to Establish Sansha City", Asia Maritime Transparency Initiative (17 April, 2017): https://amti.csis.org/chinas-plan-establish-sansha-city/.

traffic that may compound complications for Western and allied FONOPs.[390] At times, China has also utilized the Shanghai Cooperation Organisation as an organizational platform to gain support for its position, with officials from the organization explicitly proclaiming support for Chinese behavior.[391] Although several of these socialization tools have been perceived as provocative by affected actors, some have contributed to the socialization of the emerging norm's desired revisions to the principles of UNCLOS.

China's interpretation of the right of innocent passage – either as a full refutation or with the addendum that ships must receive permission – is not without precedent. Indeed, the Cold War dispute between the U.S. and the Soviet Union with regard to prior notification for ships operating in Arctic Waters may have been a key contributor to the eventual cascade of the norm underpinning the right of innocent passage.[392] Opposing perspectives on whether prior notification should apply as a caveat to the right of innocent passage persisted until 1982 when the USA and USSR issued a *Joint Statement on the Uniform Interpretation of Rules of International Law Governing Innocent Passage*:

> "All ships, including warships, regardless of cargo, armament, or means of propulsion enjoy the right of innocent passage through the territorial sea in accordance with the international law, for which neither prior notification nor authorization is required."[393]

Nevertheless, a myriad of countries have at various times advocated the right of coastal states to demand prior notification or authorization to foreign navies or differentiate innocent passage depending on territorial waters or EEZs, including Malaysia, Saudi Arabia, Oman, Morocco and Yemen.[394] Only Beijing is doing so for the entire nine-dash line, not just its EEZ, and has the weight and clout to gradually enforce it. China has thereby assumed the role as the primary norm entrepreneur in socializing these disparate sentiments into broad support for its emergent norm revising the right of innocent passage.

---

390 Haver, Zachary, "Sansha and the Expansion of China's South China Sea Administration", Asia Maritime Transparency Initiative (12 May, 2020): https://amti.csis.org/sansha-and-the-expansion-of-chinas-south-china-sea-administration/; Williams, Zachary, "China's Tightening Grasp in the South China Sea: A First-Hand Look", The Diplomat (10 June, 2020): https://thediplomat.com/2020/06/chinas-tightening-grasp-in-the-south-china-sea-a-first-hand-look/.

391 Nan, Li, "SCO Supports Peace and Stability in South China Sea", Beijing Review (24 May, 2016): http://www.bjreview.com/World/201605/t20160525_800057621.html.

392 Ergina, Natalia, "The Regulation of International Navigation Through the Northern Sea Route", The Arctic Institute of Norway, (September 2014): https://munin.uit.no/bitstream/handle/10037/7161/thesis.pdf?sequence=1.

393 Williams, Simon O., "Maritime Security: The Concept of Innocent Passage", Maritime Executive (17 December, 2014): https://www.maritime-executive.com/features/Maritime-Security-Private-The-Concept-of-Innocent-Passage.

394 Jin, Shao, "The Question of Innocent Passage of Warships: After UNCLOS III", Marine Policy 13, no. 1, (January, 1989) pp. 56-67; Reilingh, Vries, "Warships in Territorial Waters, Their Right of Innocent Passage", Netherlands Yearbook of International Law (2), (December, 1971), pp. 29-67: https://www.cambridge.org/core/journals/netherlands-yearbook-of-international-law/article/warships-in-territorial-waters-their-right-of-innocent-passage/9E960F2999F668121E3E42615ED3B4B7.

The U.S., several European states including France and the UK, and partners in the region have attempted to counter the propagation of both of these norms by employing their own socialization tools. The overarching purpose has been to socialize China, and other hesitant actors, to accept the widely recognized norm of behavior rooted in the upholding of salient UNCLOS principles, such as Freedom of Navigation and Right of Innocent Passage. The West and other litigant states in the South China Sea have sought to reaffirm and challenge China's dismissal of international law, most notably in the 2016 tribunal case of the Philippines. Vietnam has contemplated similar legal measures and regularly referred to The UN charter and UNCLOS as its basis for negotiations with Beijing.[395] This reiteration of existing law has the effect of challenging China's emergent norm, reflecting a dynamic of norm emergence by which a norm may be strengthened through repetition and reiteration by its supporters.[396] Consequently, violations of internalized norms that go unchallenged have the effect of revising the normative status quo in favor of an emergent replacement or exemption.[397] Those states seeking to reaffirm UNCLOS refer to errors in China's interpretation of international law, namely that the clause regarding territorial waters or EEZs does not apply to the artificially created islands, as well as pointing out the legal insignificance of historic rights.[398] By doing this and pointing out individual behavioral transgressions, they framed China's behavior as unacceptable.[399] However, the effectiveness of these socialization tools remains doubtful for they have not produced tangible results on the ground or mobilized more widespread defense of the internalized UNCLOS norm.

Persuasion

China has used diplomacy, mostly in the form of bilateral talks, to persuade other states to accept its emergent norm that the UNCLOS either does not apply or should be caveated with anti-access maritime clauses. The common denominator shared across the 70+ countries that have voiced varying degrees of support for China's claim stem

395 Pearson, James; Vu, Khanh, "Vietnam Mulls Legal Action Over South China Sea Dispute", Reuters, (6 November, 2019): https://www.reuters.com/article/us-vietnam-southchinasea/vietnam-mulls-legal-action-over-south-china-sea-dispute-idUSKBN1XG1D6.

396 Payne, Rodger, "Persuasion, Frame and Norm Construction", European Journal of International Relations 7, no.1, (2001): http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.525.5373&rep=rep1&type=pdf.

397 Romaniuk, Scott; Grice, Francis, "Norms, Norm Violators, and IR Theory", E-international Relations, (15 November, 2018): https://www.e-ir.info/2018/11/15/norms-norm-violations-and-ir-theory/.

398 Bader, Jeffrey, "The U.S. and China's Nine-Dash Line: Ending the Ambiguity", Brookings, (6 February, 2014): https://www.brookings.edu/opinions/the-u-s-and-chinas-nine-dash-line-ending-the-ambiguity/; Franki, Julie, "Seize the Sea: The Territorial Conflict Between the United States and China Over Military Operations in the South China Sea", Emory International Law Review (31), pp.1023-1024: https://law.emory.edu/eilr/_documents/volumes/31/recent%20developments/franki.pdf.

399 Asia Transparency Initiative, "Failing or Incomplete? Grading the South China Sea Arbitration" (11 July, 2019): https://amti.csis.org/failing-or-incomplete-grading-the-south-china-sea-arbitration/; Panda, Ankit, '5 Takeaways on China's Theft of a US Drone in Philippine Waters in the South China Sea', The Diplomat (17 December, 2016): https://thediplomat.com/2016/12/5-takeaways-on-chinas-theft-of-a-us-drone-in-the-philippine-waters-in-the-south-china-sea/; Chairman's Press, "Risch, Menendez, Gardner, Markey Comment on Chinese Coast Guard's Sinking of a Vietnamese Fishing Boat, Deployment of Military Aircraft in South China Sea", Foreign Relations (10 April, 2020): https://www.foreign.senate.gov/press/chair/release/risch-menendez-gardner-markey-comment-on-chinese-coast-guards-sinking-of-a-vietnamese-fishing-boat-deployment-of-military-aircraft-in-south-china-sea.

from a desire to avoid entanglement in a bilateral US-China standoff, and national self-interest.[400] More broadly, this sporadic support – including from countries with rival territorial claims to China – revolves around a lack of consensus on what 'China's position' is. This result is owing to Beijing's cultivated ambiguity in its 'take and talk' approach of outward willingness to peacefully negotiate. It has additionally leveraged disunity within ASEAN and the divergent interests of its members, particularly in their respective economic entanglements with China and disparate social outlooks and political priorities.[401] This lack of consensus has prevented a more unified front against China's norm violating behavior, and ceded its space to employ further persuasive incentives to stymie more robust affirmation of international law and existing norms.

These persuasive Chinese efforts to propagate its revisions to existing legal rulings and norms is most prominently shown in the disparate support for China's position in light of the 2016 international tribunal case. Countries as disparate as Thailand, Myanmar, Malaysia, Iran, Pakistan, and India voiced varying degrees of support for the Chinese position, though the exact number of countries with similar attitudes is purported to be much higher.[402] Nonetheless, it is hard to assess whether this support is the result of active persuasion on the part of China, or mere anticipation of material or immaterial potential benefits in the future, or of independently developed positions.[403]

The West and other regional countries have similarly sought to utilize persuasion to promote the maintenance of the existing norm rooted in UNCLOS principles. Most active efforts in this direction stem from the continual diplomatic talks aimed at establishing a Code of Conduct in the South China Sea Context, though without tangible results so far.[404] Additionally, the diplomatic efforts of individual states have also pursued this persuasive logic; the U.S. and Australia, for example, have diplomatically supported both China and ASEAN in reaching the Code of Conduct

400 Wen, Wang; Xiaochen, Chen, "Who Supports China in the South China Sea and Why", The Diplomat (27 July, 2016): https://thediplomat.com/2016/07/who-supports-china-in-the-south-china-sea-and-why/.

401 O'Neill, Daniel, "Dividing ASEAN and Conquering the South China Sea: China's Financial Power Projection", Hong Kong University Press, (September, 2018), p.41.

402 Dutton, Peter, "Cracks in the Global Foundation: International Law and Instability in the South China Sea", in "Cooperation From Strength: The United States, China and the South China Sea", (1 January, 2012): https://www.jstor.org/stable/resrep06426?seq=1#metadata_info_tab_contents; AMTI Leadership, "Arbitration Support Tracker', Asia Maritime Transparency Initiative", (16 June, 2016): https://amti.csis.org/arbitration-support-tracker/; Wen, Wang; Xiaochen, Chen, "Who Supports China in the South China Sea and Why", The Diplomat (27 July, 2016): https://thediplomat.com/2016/07/who-supports-china-in-the-south-china-sea-and-why/; PTI, "South China Sea Dispute: China Claims Support of 40 Countries", Economic Times, (12 July, 2018): https://economictimes.indiatimes.com/news/defence/south-china-sea-dispute-china-claims-support-of-40-countries/articleshow/52363836.cms?from=mdr.

403 There are dozens of countries advocating for some form of constrain on navigation, though not necessarily in the same form as China; see Pham, Trand; Truong-Minh Vu, "From Clash of Vision to Power Struggle: The US, China, and Freedom of Navigation", E-International Relations (31 October, 2014): https://www.e-ir.info/2014/10/31/from-clash-of-vision-to-power-struggle-the-us-china-and-freedom-of-navigation/.

404 AFP-JIJI, "Beijing Says it is Ready to Work With ASEAN on South China Sea Code of Conduct", Japan Times (3 November, 2019): https://www.japantimes.co.jp/news/2019/11/03/asia-pacific/politics-diplomacy-asia-pacific/beijing-says-ready-work-asean-south-china-sea-code-conduct/#.XuY69kUzZPY.

agreement.[405] These efforts seem to have had some effect; The 36th ASEAN summit in Hanoi issued a joint statement which "reaffirmed that the 1982 UNCLOS is the basis for determining maritime entitlements, sovereign rights, jurisdiction and legitimate interests over maritime zones".[406] These efforts have sought to cool rising U.S.-China tensions, offering bilateral and multilateral engagement as an alternative to FONOPs as the centerpiece for countering China's assertions.[407] Taiwan, for example, has also proposed plans for achieving stability in the region within the framework of the South China Sea Peace Initiative.[408] The persuasive tools used by this side have produced limited results, mostly in the form of joint declarations and promises, but with no change to realities on the ground.

Coercion

China has utilized coercion jointly alongside its socialization and persuasion tactics in propagating its emergent norm.[409] These measures occur mostly through military and economic inducements to enforce both aspects of the emerging norm.[410] Beijing has repeatedly used force or threats of force, both covertly and overtly, in defense of its claims.[411] While China's continuous and swift development of its blue water navy enables it to increasingly project power further away from its shores, it has mostly relied on law enforcement activities to propagate the EEZ-violating norm, masquerading its efforts as an enforcement of Chinese domestic law to bolster its claims rather than as a challenge to international maritime law.[412] The incorporation of the Woody, Spratly and Paracel Islands as city districts brings its own coercive element, as alongside increased administrative control China has introduced robust military and coastguard capabilities to bolster its presence in the area.[413] While not coercive per se, China has sought to further normalize its maritime presence through joint-military exercises,

405 Starting, Rebecca, "Australia's Approach to the South China Sea Dispute", East-West Center (24 July, 2019): https://www.eastwestcenter.org/publications/australia%E2%80%99s-approach-the-south-china-sea-disputes; Cihang, Chen, "The U.S. Policy on the Code of Conduct in the South China Sea", The Journal of International Studies 39(4), (August, 2018): http://jtp.cnki.net/bilingual/detail/html/GJZY201804003.

406 Associated Press, "ASEAN Leaders Cite 1982 UN Treaty in South China Sea Dispute", Guardian (27 June, 2020): https://www.theguardian.com/world/2020/jun/27/asean-leaders-cite-1982-un-treaty-in-south-china-sea-dispute.

407 Li, Chien-pi, "The South China Sea Peace Initiative in a Transitional Security Environment", American Journal of Chinese Studies 23, no. 1, (July, 2016): https://www.jstor.org/stable/44289143?seq=1.

408 Tsai, George, "Taiwan and Its South China Sea Peace Initiative", The Diplomat (28 August, 2015): https://thediplomat.com/2015/08/taiwan-and-its-south-china-sea-peace-initiative/.

409 Corr, Andrew, "China's Take-and-Talk in the South China Sea." Forbes, (March 29, 2017): https://www.forbes.com/sites/anderscorr/2017/03/29/chinas-take-and-talk-strategy-in-the-south-china-sea/#69887aa33216.

410 Green et al., "Countering Coercion in Maritime Asia", pp. 51–262.

411 Van Pham, "The Use or Threat of Force in the South China Sea Disputes Since 1945: A Timeline", Power Politics in Asia's Contested Waters (20 February 2016): https://link.springer.com/chapter/10.1007/978-3-319-26152-2_25.

412 Corr, Anders, "China's Take-And-Talk in the South China Sea", Forbes (29 March, 2017): https://chinapower.csis.org/maritime-forces-destabilizing-asia/.

413 Haver, Zachary, "Sansha and the Expansion of China's South China Sea Administration", Asia Maritime Transparency Initiative, (12 May, 2020): https://amti.csis.org/sansha-and-the-expansion-of-chinas-south-china-sea-administration/.

such as the 2018 trilateral Peace and Friendship naval exercises with Malaysia and Thailand, as part of efforts to soothe regional tensions.[414]

These actions reflect China's hardline outlook on issues it perceives as central to its sovereignty. President Xi has linked sovereignty with the accomplishment of his 'China Dream', proclaiming that "no foreign country should expect us to trade away our core interests" or expect China "to swallow the bitter fruit" of encroachment upon its "sovereignty".[415] More recently, in 2018, Xi Jinping commented to U.S. Secretary of Defense James Mattis that China "cannot lose even one inch of the territory left behind by our ancestors".[416] In this respect, China regularly employs coercive tactics against its neighbors in asserting its territorial claims, ranging from coastal patrols to the actual sinking of fishing vessels - as occurred most recently in the case of a Vietnamese fishing vessel rammed by a Chinese surveillance ship.[417] A major facet of China's coercive measures on the ground are patrols by the People's Armed Forces Maritime Militia (PAFMM), a civilian reserve force employed as part of China's broader military strategy that sees "confrontational operations short of war as an effective means of accomplishing political objectives".[418]

Additionally, strong economic entanglement between China and other states also conveys the potential for economic coercion and the mere anticipation of said coercion may be sufficient for some Western and regional states to abstain from taking active countermeasures.[419] Indeed, it has been observed that recently China has relied on economic and law enforcement coercion more often than its military measures.[420] This preference for economic coercion iterates Beijing's preference for tools of influence that fall below the threshold of the use of force, a strategic choice which it employs as a

414 Parameswaran, Prashanth, "What's in China's Military Exercise With Malaysia and Thailand?", The Diplomat, (17 October, 2018): https://thediplomat.com/2018/10/whats-in-chinas-military-exercise-with-malaysia-and-thailand/.

415 Fravel, Taylor, "China's Sovereignty Obsession", Foreign Affairs, (26 June, 2020): https://www.foreignaffairs.com/articles/china/2020-06-26/chinas-sovereignty-obsession.

416 CGTN, "Xi Tells Mattis China Won't Give Up 'One Inch' of Territory", (2018): https://news.cgtn.com/news/3d3d514d3545444e78457a6333566d54/share_p.html.

417 Vu, Khanh, "Vietnam Protests Beijing's Sinking of South China Sea Boat", Reuters (4 April, 2020): https://www.reuters.com/article/us-vietnam-china-southchinasea/vietnam-protests-beijings-sinking-of-south-china-sea-boat-idUSKBN21M072.

418 United States Office of the Secretary of Defense, "Annual Report to Congress – Military and Security Developments Involving the People's Republic of China 2019", Department of Defense, (2 May, 2019): https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

419 Luc, Tuan Anh, "Decoding Australia's Strange Silence Over China's Transgressions in the South China Sea", The Diplomat (15 August, 2019): https://thediplomat.com/2019/08/decoding-australias-strange-silence-over-chinas-transgressions-in-the-south-china-sea/; Ravindran, Madhu Sudan (2012), "China's Potential for Economic Coercion in the South China Sea Disputes: A Comparative Study of the Philippines and Vietnam", Journal of Current Southeast Asian Affairs, 31, no. 3, pp. 105-132.

420 Zhang, K., "Cautious Bully: Reputation, Resolve, and Beijing's Use of Coercion in the South China Sea" International Security 44, no. 1, (2019), pp.117–159: doi:10.1162/isec_a_00354.

general principle in its 'talk and take' approach.[421] Though the use of coercive tools has not yet led to the cascade or internalization of Chinese propagated norms in violation of UNCLOS principles, it has undermined the latter and influenced individual actors to abstain from taking more resolute countermeasures to maintain the incumbent norm.

The West and some other regional states have largely used active and passive tools of military coercion to propagate the pre-existing norm respecting the UNCLOS principles. The repeated conduct of FONOPs can be interpreted as a form of coercion whose purpose is the promotion of that pre-existing norm.[422] Furthermore, the military buildup of anti-access and area-denial bubbles, particularly on the side of Vietnam and the U.S., also has the potential to produce coercive effects.[423] Overall, the effectiveness of these coercive tools has fallen short as only a handful of countries partake in the reaffirmation of the existing UNCLOS norms, and their employment has not led to a Chinese change in behavior as president Xi is unlikely to budge for the U.S. or any other non-regional interference.

This case study shows the interactive dynamics between the promotion of emerging norms versus the defense of the previously internalized ones. Though both China and its opponents have used socializing, persuasive and coercive efforts to promote their normative behavior, the results remain inconclusive at best or favorable to China at worst. The emerging norm in violation of UNCLOS has not cascaded nor has it been internalized by other actors.

Second-Order Normative Effects of the Countermeasures

The second order effects of U.S. countermeasures may incite escalation and legitimization of Chinese behavior. The second-order normative effects of FONOPs is considered to be limited because its mandate is enshrined within UNCLOS and customary international law. The credibility of American FONOPs may be undermined by the fact that the U.S. has not ratified UNCLOS. Furthermore, FONOPs have been interpreted as a provocation by China.[424] This is so because China perceives these

421 Hicks, Kathleen; Shah, Hijab; Federici, Joseph; Akca, Asya; Sheppard, Lindsey, "By Other Means Part I: Campaigning in the Gray Zone", CSIS (8 July, 2019), p.35: https://books.google.nl/books?id=28SrDwAAQBAJ&pg=PA7&lpg=PA7&dq=china+tools+of+influence+threshold+use+of+force+economic+coercion&source=bl&ots=QNfP5dvAEk&sig=ACfU3U0A1tFkY-ANVWfUG5jq4ZHl5t5R7Q&hl=en&sa=X&ved=2ahUKEwjv9PzQmKnqAhXB2qQKHTBpCw0Q6AEwAHoECAoQAQ#v=onepage&q=south%20china%20sea&f=false.

422 Lan, NGO Di, "The Usefulness of "Redundant" Freedom of Navigation Operations", Asia Maritime Transparency Initiative, (26 January, 2018): https://amti.csis.org/usefulness-redundant-fonops/.

423 Bonds, Timothy; Predd, Joel; Heath, Timothy; Chase, Michael; Johnson, Michael; Lostumbo, Michael; Bonomo, James; Mane, Muharrem; Steinberg, Paul, "What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?", RAND (2017): https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1820/RAND_RR1820.pdf.

424 Reuters, "China Urges United States to Stop Provocative Acts in South China Sea" (22 November, 2019): https://www.reuters.com/article/us-usa-china-southchinasea-fonop/china-urges-united-states-to-stop-provocative-acts-in-south-china-sea-idUSKBN1XW07P.

operations as constituting a threat to its sovereign rights over the area.[425] Regular employment of FONOPs can feed the Chinese narrative that more control is required to bar U.S. and other powers outside of the region from pursuing their foreign policy goals in the South China Sea.[426] In sum, the use of FONOPs may have created perceived domestic legitimacy for Chinese military buildup in the area as well as encouraged potential escalation of the conflict.

3.5.4 Key Takeaways

Firstly, both China and the U.S. have employed a combination of socialization, persuasion and coercion to propagate and cultivate respective norms, either seeking to reaffirm or revise the normative status quo. China's socialization efforts have shown promising initial signs; it has gained vocal and formal sympathies from actors such as Russia, Thailand, Myanmar, Malaysia, Iran, Pakistan, and India. It thereby challenged customary international law and the primary maritime security framework without ample disapproval and resistance from the international community. China has effectively propelled the rise of a revisionist emergent norm through the coercive leveraging of its neighbors' economic entanglements, persuasive incentives through setting a precedent for newly permissible actions and exploiting social and political divisions through linking and framing. In sum, it seems that the norm conflict currently hinges upon China's calculation of its gains in continuing to promote its position as a norm entrepreneur, relative to the reciprocal costs in challenging the normative status quo and the willingness of incumbent norm leaders to defend it. As of now, the established UNCLOS norm remains the more widely internalized norm, albeit under constant challenge by China's emergent rival interpretation, which may spillover to other emerging great powers, such as India.

By contrast, joint countermeasures – particularly those centered on U.S. FONOPs – have done little to challenge the substance of China's claims. Chinese persuasive efforts have shown promising signs in gathering support and silencing opposition for their claims in the South China Sea and the challenge to UNCLOS norms on freedom of navigation. By contrast, the latter effort has produced little more than the vague prospects of establishing a Code of Conduct in the South China Sea, a move that China is likely to deflect through continued 'talk and take' tactics. These tactics and its political system allow the Chinese to take a long-term strategy through which they meet their objectives through-steps, which become major strides over time. Chinese use of coercion through law enforcement, militia, and PLA operations has propagated

425 Xinjun Zhang, "The Latest Developments of the US Freedom of Navigation Programs in the South China Sea: Deregulation or Re-Balance?", Journal of East Asia and International Law 9, no. 1 (2016): pp.167–82.

426 Urchick, Daniel, 'Tensions in the South China Sea National Intelligence Estimate: The Next Two to Three Years', Small Wars Journal (20 February, 2017): https://smallwarsjournal.com/jrnl/art/tensions-in-the-south-china-sea-national-intelligence-estimate-the-next-two-to-three-years.

its emerging norm in spite of UNCLOS principles and, perhaps equally importantly, has silenced some regional voices in opposition to the norm. Comparatively, coercive tools employed by the U.S. and other regional states have not contributed to the further cultivation of pre-existing norms. In sum, the effectiveness of individual tools of propagation has heavily favored China, especially in its use of coercive and persuasive influence tools.

Finally, the risks flowing from the second-order normative effects produced by FONOPs are relatively low. Instead, they present operational side-effects that could justify Chinese assertiveness in the region and potentially escalate the conflict. Alternatively, the lack of tangible effects produced by FONOPs may signal weakness and lack of credibility on the U.S. side. These negative effects effectively place the U.S., and the West in general, in choosing between two unenviable options, in which both acting and not acting may damage its long-term interests.

3.6 Insights Derived from Case Studies

The analysis of norm development across five different cases yields a better understanding of the strategies, tools of influence, dilemmas and trade-offs by European states and the U.S. in their response to Russian, Chinese, and ISIS hybrid operations. Two of the five cases show the different strategies that were used to actively promote the emergence of international norms with some degree of success. Two other cases highlight two potential areas for establishing a norm. A fifth case highlights how seemingly fully internalized norms are challenged. Below, we briefly highlight five key insights that emerge from the analysis of each of the five cases.

First, a norm to protect electoral infrastructure from cyber operations emerged from the broad range of U.S. and European countermeasures. Whilst the norm is in its early stages of the lifecycle, the strategies and tools of influence used by the entrepreneurs can be described as pluralistic, meaning that they intend for the norm to be spread and internalized using multiple tools of influence simultaneously. In its early stages, multiple state and transnational NGO entrepreneurs *persuade* others by *framing* the norm to larger issues such as the threat to democracy and sovereignty from malign state and non-state actors, and by *linking* it to well-established norms on nonintervention and critical infrastructure protection. Linking and framing a norm as an enhanced interpretation of existing norms can be seen as a tactical bargaining tool to persuade like-minded countries, such as the U.S., that rather focus on implementing previously agreed UN cyber-norms over creating new norms. This reinforces the belief that often the best path to support the acceptance of existing norms is to agree on new add-ons to reinforce existing ones. Additionally, coercion of Russia via diplomatic expulsions, sanctions and indictments, as well as socialization of the norm with like-minded

parties via organizational groups such as the GCSC, Paris Call, and the UN, coupled to further the norm alongside coercive socialization measures to stigmatize Russia via naming and shaming.

Similarly, U.S. indictments and the threat of sanctions, as well as persuasion (better Sino-American relations) showed promising results of Chinese internalization of an emerging norm against economic espionage as it led to the most significant, albeit short-lived, reported drop in Chinese IP theft. If we consider the resurgence of Chinese IP theft a result of souring US-China relations under the Trump administration, we can conclude that the persuasive incentives taken by the U.S. to push towards Chinese adherence and internalization have disappeared. Simultaneously, the U.S. changed its coercion strategy away from targeting specific norm violators, towards a broader bilateral trade and tariff war. Chinese policymakers now have little to gain from continuing to honor the norm as bilateral relations worsen regardless. Furthermore, the sweeping sanctions against China, in combination with the tariffs the U.S. levies on its partners isolates the norm violation and the threat of IP theft as a bilateral US-China issue. Instead, the development of the norm may be better served if the U.S. were to mobilize large-scale, coordinated attribution and subsequent sanctions *with* its partners – other victims that have struck similar norms with China, such as Canada, Australia, the UK, or Germany – in the same coordinated fashion as the countermeasures adopted against Russian hacking of democratic institutions. While China may initially have appeared to adhere to the norm, not because of its content but as part of tactical bargains, that serve their interests in response to incentives or coercion, norm internalization or compliance may still become routinized as habits take hold. Furthermore, it may become entrapped by the reciprocal consequences of insincere prior rhetorical commitments in ways that push towards norm conformity and potential acceptance. The alternative is the danger of appearing hypocritical, which would come with reputational and credibility costs.

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

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

Third, despite norms being traditionally instruments that govern peacetime operations, our normative analysis of U.S. wartime countermeasures against ISIS reaffirmed the principles of International Humanitarian Law (IHL) being fully applicable to cyber and influence operations. Against this backdrop, we explored the possibility of establishing a normative yardstick for truth in 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 yet, in part because of the clandestine nature of information operations, because the course of action is not yet strong enough to be labeled as habitual, and partly because they occur in wartime. Instead, the principle value of this inception norm resides in the way U.S. countermeasures in the information environment that are conducted during wartime against a non-state entity, compare with the previous case examination of a peacetime response to Russian disinformation, and the evolving overlap therein. 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 engages in disinformation and propagation across broad public media channels without regard for their collateral damage, as evidenced in the previous case study. On the other hand, the need for such a norm may become more evident as these wartime measures are migrated to a peacetime environment.

Fourth, the Chinese reinterpretation of the innocent passage and freedom of navigation norm embedded in UNCLOS and customary international law shows that the formation of a fully internalized norm does not imply that the end product will

remain fixed or unchallenged. Instead, they evolve as the interests, context, identity, and propriety change around them. Chinese assertiveness in the South China Sea based on inchoate territorial and maritime claims, in turn, have shaped the contours and content of these norms. Beijing not only challenges how states lay claim to maritime zones but also campaigns for a revisions norm that challenges the right of innocent passage of foreign navies by barring them or by requiring previous authorization. This emerging norm is in conflict with the pre-existing norm that is enshrined in UNCLOS and customary international law and internalized by the majority of states around the world. In doing so, it undermines the only global maritime security framework and the existing balance of coastal state rights and international rights of freedom of navigation through its use of various tools of influence. States that violate widely established or internalized norms are likely to be met with punitive action and stigma from the international community. Yet punitive action has been ineffective in shaping Chinese behavior towards conformation of the pre-established norm. Similarly, China's ability to dismiss international legal rulings against it present a direct normative challenge that, if ignored, begins to routinize norm-breaking behavior. Regionally, this ineffectiveness can be explained by the power considerations, both in economic and (para)military terms, of China vis-à-vis its neighbors. Globally, the power asymmetries of the liberal international order, of which UNCLOS is a part of, is diffusing away from the West towards the East, predominately China, which is endowed with greater leeway to contest and reevaluate norms they were previously held to in a primarily European-American derived system.

In addition to the specific insights for each of the cases, the cases combined also demonstrate that a better understanding of how norms are developed to shape adversarial behavior in hybrid conflict should take into account second-order normative effects of a state's pursuit of norm-enforcing behavior. Countermeasures can trigger second-order normative effects that are too often ignored. 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 or affect socialization that keeps otherwise non-abiding actors in adherence with the overall normative status quo. Figure 1 maps the countermeasures in terms of coerciveness and their second-order normative effects. Overall, the countermeasures that were least coercive, such as public attribution, naming and shaming, indictments, and diplomatic sanctions, created second-order effects with a lower risk impact that can be mitigated. Coercive countermeasures, on the other hand, led to more impactful effects that could risk the long-term strategic interests of a state. An additional distinction can be made between the impact of *overt* and *covert* coercive measures. The overt coercive peacetime measures considered in this case, such as the U.S. pre-deployment in Russian critical infrastructure and their kinetic cyber effects against the Russian troll factory, produced higher second-order normative effects than the coercive wartime measures. After all, the overt coercive U.S. measures led had the highest second-order normative effect,

most notable on the weaponization of information and in introducing a norm of mutually assured debilitation. This does not mean that all overt coercive measures automatically create high-risk second-order normative effects, but are instead more likely to. The consideration of these effects should enhance policy-oriented discussion to make a more informed and conscious decision on countermeasures that takes the unintended normative consequences into consideration.

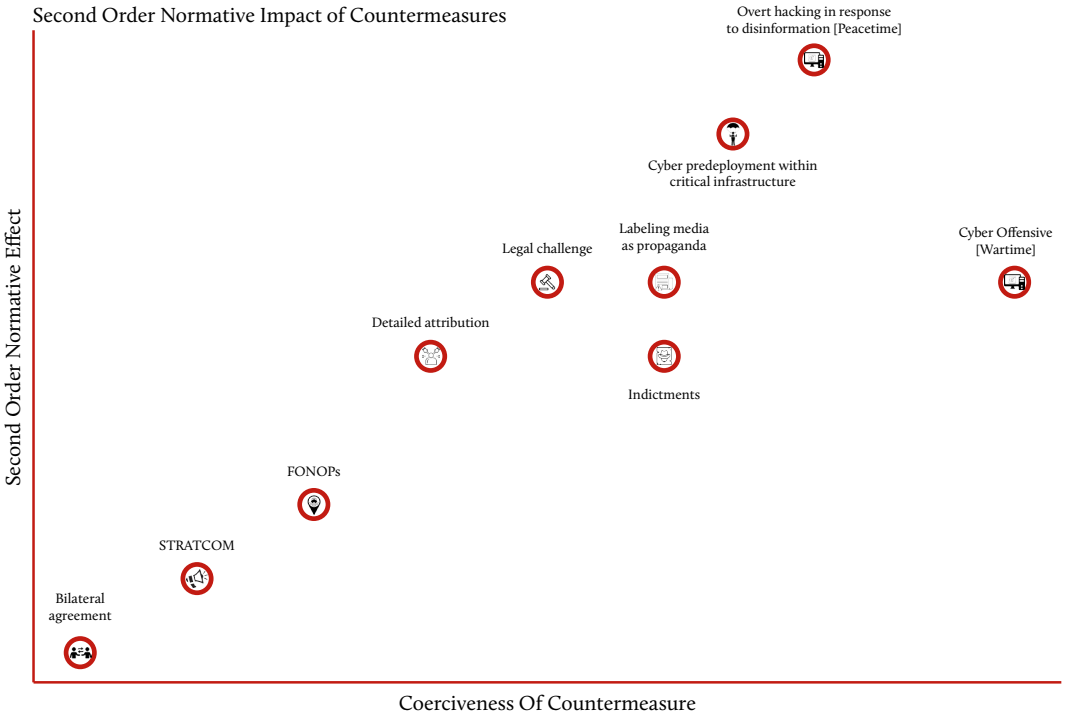

Figure 1: Second Order Normative Effects of Countermeasures