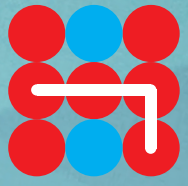
RESEARCH AND ANALYSIS

Hybrid CoE Trend Report 3

APRIL 2020

Hybrid threats and the law: Concepts, trends and implications

AUREL SARI



Hybrid CoE

Hybrid CoE Trend Report 3

Hybrid threats and the law: Concepts, trends and implications

AUREL SARI

Hybrid CoE Trend Reports are an outcome of expert-pool meetings on a given theme. They highlight the main trends of the theme, provide multiple perspectives on current challenges as well as academic discourse on the topic, and serve as background material for policymakers. They aim to distinguish between what really constitutes a threat, what appears to be a threat but is not necessarily one, and what has the potential to become one. Hybrid CoE's Research and Analysis engages expert pools on relevant themes in the landscape of hybrid threats.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-39-7
ISSN 2670-1804

April 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland.

Contents

Foreword

The European security environment is becoming increasingly hybrid in nature. In addition to the traditional military domain, security threats are trickling down to all aspects of social life. Democratic states are threatened by actors who are willing and more able than ever before to attack domains not perceived to belong to the core field of security with multiple tools in creative combination to reach their goals and advance their strategic interests in unacceptable ways.

Analysing emerging trends related to security and highlighting long-term undercurrents will help us to understand the changing security environment and be better prepared to respond to potential hybrid threats in the future. Being able to read trends allows us to place current events into context and helps us to distinguish between what is a threat, what looks like but is not necessarily a threat, and what has the potential to become a threat in the future.

The European Centre of Excellence for Countering Hybrid Threats operates expert pools to support its participating states and the activities of the Centre's Communities of Interest. The expert pools work as a venue for exchanging information, building connections and gaining a comprehensive understanding of the trends under a specific theme. These trends are then linked, through Hybrid CoE, to potential hybrid threats. The expert pools are an ongoing process and provide content for the Centre's work.

Engaging with the expert pools and the activity relating to them is in line with Hybrid CoE's founding memorandum of understanding, which states that Hybrid CoE is to act as a hub of expertise, to offer collective competence and to encourage strategic-level dialogue. This activity should be multidisciplinary and academic-based. Thus, the purpose of engaging with the expert pools is not to pursue a single truth, but rather to provide multiple perspectives on current challenges, to provide perspectives on the academic discourse on the topic, and to serve as a background for policymakers. The added value of this work is that it examines the subject from a hybrid threat perspective. Each participating state, the EU and NATO can then consider which facets of knowledge will be most useful for it from its own perspective.

Introduction

Almost three decades ago, the end of the Cold War generated a sense of optimism that great power competition and ideological divisions would give way to a more cooperative, democratic and liberal world order.[1] This optimism proved short-lived: civil wars, state failure and ethnic cleansing wrecked hopes for a more peaceful international system. Despite these setbacks, the belief that international institutions could provide a framework for great power rapprochement persisted. More recent developments have shaken that faith.[2]

Over the last decade, the world has entered into a period where the great powers are prepared to assert their interests in a more antagonistic manner. Russia has violated one of the fundamental principles of the post-war international order, the rule against the acquisition of another State's territory through the use of force, when it occupied and annexed Crimea.[3] China is asserting its interests more vigorously, claiming parts of the South China Sea and declining to accept the award rendered against it in this matter by the Permanent Court of Arbitration.[4] Simultaneously, support for multilateralism is waning. Recent withdrawals from international institutions and agreements, such as the departure of the Philippines from the International Criminal Court and the renunciation of a string of treaties by the United States, including the Iran nuclear agreement, are symptomatic of a growing disillusionment with international norms and processes. Indeed, it seems that the continued full support for a rules-based international order by some of its traditional champions can no longer be taken for granted.[5]

This turn towards more open confrontation and greater unilateralism has come at a time of major technological developments. Technological progress has put greater destructive power than ever before into the hands of non-State actors. It has also opened up new avenues for foreign interference and subversion in the form of fake news, election meddling and cyber espionage. As a result, modern societies have become more vulnerable to acts of terrorism and to hostile influence and intervention.

Overall, two mutually reinforcing trends are at work here: strategic competition has become more intense and has taken on novel forms, aided by new technologies, while the norms, institutions and processes intended to keep geopolitical rivalry in check have come under increasing pressure, to the risk of unravelling.

To some, these developments merely demonstrate that the idea of a rules-based international order is an illusion. Great powers have always prioritised the national interest over international rules and will continue to do so. To others, these developments are a cause for redoubling efforts to strengthen multilateralism.

What is beyond doubt is that these trends pose significant challenges to the international rule of law. The turn to greater antagonism has brought selective compliance and serious violations of fundamental principles of international law. The use of new technologies and platforms, including cyber and social media, has raised difficult questions about how the existing rules apply in these fields. Adherence to international norms by law-abiding societies has created vulnerabilities that less scrupulous players are able to exploit. Meanwhile, key actors pursue competing visions of international order: transactionalist approaches compete with multilateralism, while liberal ideals clash with sovereignty-focused Statism.

1 See, famously, Francis Fukuyama, *The End of History and the Last Man* (Free Press, New York, 1992).
2 Alison Pert, 'International Law in a Post-Post-Cold War World—Can It Survive?' (2017) 4 *Asia and the Pacific Policy Studies* 362.
3 See Thomas D. Grant, *Aggression against Ukraine: Territory, Responsibility, and International Law* (Palgrave Macmillan, Basingstoke, 2015).
4 'Statement of the Ministry of Foreign Affairs of the People's Republic of China on the Award of 12 July 2016 of the Arbitral Tribunal in the South China Sea Arbitration Established at the Request of the Republic of the Philippines' (2016) 15 *Chinese Journal of International Law* 905. See Permanent Court of Arbitration Case No 2013-19, *South China Sea Arbitration (Philippines v. China)*, Award of 12 July 2016.
5 Doug Stokes, 'Trump, American Hegemony and the Future of the Liberal International Order' (2018) 94 *International Affairs* 133.

For all these reasons, today, the content, meaning and application of international rules is fiercely contested — not just among States, but by a growing number of actors in a wide range of fora, including in the information sphere. International law has emerged as a critical subject, instrument and domain of strategic contestation.

It is against this background that the Research and Strategic Analysis team at the Hybrid Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) held a workshop at the University of Exeter in April 2019 to identify the key trends affecting national and international legal resilience in an era of hybrid threats. The trend-mapping undertaken at this workshop was the first step in a project designed to assess and address potential legal vulnerabilities that could be exploited by hostile actors.

Prior to the workshop, experts from a variety of backgrounds were asked to provide a brief outline of the legal trends they consider most important in their field. As a result of these written contributions and the discussions held at the workshop itself, the Hybrid CoE Research and Strategic Analysis team identified the following themes and trends that affect the legal resilience of our societies:

- law as a strategic instrument
- law as a hybrid threat
- legal grey areas
- legal fault lines and interfaces.

The remaining sections of this report explore these themes and trends in greater detail. They are meant neither as a definite study of the subject nor as an exhaustive list of the legal challenges that the current security environment presents. Rather, they are offered as food for thought and to provide direction for further work.

Law as a strategic instrument

States and other international actors use law as an instrument for pursuing their strategic interests. They do so in a variety of ways.

States employ domestic and international law to regulate the conduct of third parties and to sanction them if they fail to comply with the applicable rules. Law in this regulatory function involves the exercise of coercive power. For example, in May 2015, Russian President Vladimir Putin signed an act that authorises the Prosecutor General of the Russian Federation to designate certain foreign and international non-governmental organisations as 'undesirable' and to ban them from operating in Russia.[6] The law has been used in conjunction with other legislative measures to curtail the work of civil and human rights organisations. As a result, it is widely seen as an attempt to supress civic activism and to silence voices critical of the Russian government.[7] In 2019, the first criminal proceedings under the law were brought against Anastasia Shevchenko, a human rights and pro-democracy activist.[8]

China does not shy away from relying on its regulatory authority to assert its strategic interests either. Following North Korea's successful satellite launch in February 2016, South Korea decided to proceed with procuring a Terminal High Altitude Area Defense (THAAD) ballistic missile-defence battery from the United States. China immediately expressed strong opposition to the deployment, arguing that the system's advanced radar technology weakened its nuclear deterrence and exceeded South Korea's legitimate defence requirements. China also launched a campaign of economic retaliation,[9] including measures targeting the business interests of Lotte, a South Korean company active in China. Lotte had provoked the ire of the Chinese authorities by agreeing to cede one of its golf courses to the South Korean government to serve as the deployment site for the THAAD system.[10] According to reports, the Chinese authorities launched investigations into Lotte's activities in China, fined the company for its advertising practices and forced it to shut down most of its department stores for alleged violations of Chinese fire-code regulations. By mid-2018, Lotte closed all of its department stores in China for good.

States and other actors also rely on the law to justify their own conduct. Law serves as a basis for principled action. Acting in compliance with the rules constitutes a source of legitimacy. This is why governments rarely admit to breaking the law, tending instead to mask their non-compliance as best as they can, even when they are unashamedly flouting the applicable rules. Russia's annexation of Crimea illustrates the point. Responding to accusations that taking control of Crimea violated international law, President Putin suggested in March 2014 that Russian troops were present on the Crimean peninsula in accordance with pre-existing bilateral agreements in force between Russia and Ukraine.[11] This much is true. But the deployment of those troops outside their military bases without the consent of the Ukrainian authorities, let alone their reinforcement with additional units to bring the peninsula within the control of Russia,

6 Федеральный закон от 23.05.2015 № 129-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации [Federal Law of 23 May 2015 No 129-FZ On Amending Certain Legislative Acts of the Russian Federation] (http://publication.pravo.gov.ru/Document/View/0001201505230001).
7 Maria Lipman, 'At the Turning Point to Repression' (2016) 54 *Russian Politics & Law* 341. See also Geir Flikke, 'Resurgent Authoritarianism: The Case of Russia's New NGO Legislation' (2016) 32 *Post-Soviet Affairs* 103.
8 Vladimir Kara-Murza, 'The Kremlin Deploys its New Law against "Undesirables"', *The Washington Post*, 25 January 2019.
9 Ethan Meick and Nargiza Salidjanova, *China's Response to U.S.-South Korean Missile Defense System Deployment and its Implications* (US-China Economic and Security Review Commission, Washington, DC, 2017).
10 'Thaad's all, Folks; Lotte Exits China', *The Economist*, 21 October 2017.
11 Address by the President of the Russian Federation, 18 March 2018 (http://en.kremlin.ru/events/president/news/20603).

was a manifest and entirely unambiguous violation of those agreements.[12] Similarly, Russian Foreign Minister Sergey Lavrov denied that the annexation of Crimea violated the assurances that Russia gave to Ukraine in the Budapest Memorandum of 1994.[13] According to Lavrov, the only legally binding commitment that Russia had assumed in the Memorandum was not to use or threaten to use nuclear weapons against Ukraine.[14] While Russia did not contravene this commitment, Foreign Minister Lavrov's denial overlooks the fact that Russia also agreed to 'respect the independence and sovereignty and the *existing* borders of Ukraine',[15] a commitment that Russia most emphatically failed to honour.[16]

In addition, States and non-State actors rely on the law as a means for censuring their opponents and contesting the legitimacy of their actions. In an era where compliance with the law is a critical source of legitimacy,[17] casting doubt on the legality of an adversary's conduct is a powerful method for delegitimising him in the eyes of international and domestic audiences. Since the rule of law is meant to apply to everyone in equal measure, a weaker party may invoke the law against a more powerful opponent with relative ease, thus providing it with an asymmetric advantage. While this is a virtue of the law and not a flaw, experience shows that unscrupulous actors confronting law-abiding ones can press this advantage further, as Hezbollah and Hamas regularly do against Israel. Given the military and technological superiority of Israel, even highly capable actors such as Hezbollah and Hamas have no realistic prospect of prevailing against Israeli forces on the battlefield. Both organisations therefore wage sophisticated information campaigns to undermine public support for Israel, to discredit its actions and to constrain its strategic options. A key component of these campaigns is the manipulation of civilian suffering and casualties in a way that portrays the State of Israel as in serious breach of its international obligations. During the Second Lebanon War, Hezbollah embedded its military positions in civilian areas and aggressively exploited reports of civilian destruction and casualties caused by the fighting, ultimately turning international opinion against Israel.[18] Using similar tactics, Hamas deliberately incurs friendly civilian casualties and uses civilians to shield its military assets and operations.[19] During the 2014 Gaza conflict, Hamas repeatedly conducted military attacks from in or near hospitals, schools and places of worship, both to shield its operations and to invite civilian collateral damage for information warfare purposes.[20] More recently, Hamas instigated violent clashes along the Gaza-Israel border and leveraged images of casualties to feed the perception that Israeli troops were using lethal force indiscriminately and disproportionately against unarmed civilians.[21]

States often invoke the law to justify their own action and to denounce their adversaries in one breath. For example, the United States justified the killing of Iranian Major General Qasem Soleimani on 2 January 2020 as an exercise of the inherent right of self-defence 'in response to an escalating series of armed attacks in recent months by the Islamic Republic of Iran and Iran-supported

12 Grant (note 3), 47. See Note verbale dated 2 March 2014 from the Permanent Mission of Ukraine addressed to the Acting Secretary-General of the Conference on Disarmament transmitting a non-paper on violations of Ukraine's laws in force and of Ukrainian-Russian agreements by military units of the Black Sea fleet of the Russian Federation on the territory of Ukraine, CD/1976, 10 March 2014.
13 Memorandum on Security Assurances in connection with Ukraine's Accession to the Treaty on the Non-Proliferation of Nuclear Weapons, 5 December 1994, UNTS No. 52241.
14 Foreign Minister Sergey Lavrov's statement and answers to questions at a joint news conference following talks with Minister of Foreign Affairs and Cooperation José Manuel García-Margallo of Spain, Moscow, 10 March 2015 (https://www.mid.ru/en/posledniye_dobavlnenniye/-/asset_publisher/MCZ7HQuMdqBY/content/id/1089618).
15 Article 1, Budapest Memorandum (note 13) (emphasis added).
16 For a more detailed analysis of Russia's legal arguments and rhetoric to justify its annexation of Crimea, see Christopher J. Borgen, 'Law, Rhetoric, Strategy: Russia and Self-Determination before and after Crimea' (2015) 91 *International Law Studies* 216; Thomas Ambrosio, 'The Rhetoric of Irredentism: The Russian Federation's Perception Management Campaign and the Annexation of Crimea' (2016) 27 *Small Wars and Insurgencies* 467.
17 See David Kennedy, *Of War and Law* (Princeton University Press, Princeton, 2006).
18 Gemunder Center for Defense and Strategy Hybrid Warfare Task Force, *Israel's Next Northern War: Operational and Legal Challenges* (Jewish Institute for National Security of America, Washington, DC, 2018), 30–33.
19 NATO Strategic Communications Centre of Excellence, *Hybrid Threats: A Strategic Communications Perspective – Annex of Case Studies* (NATO Strategic Communications Centre of Excellence, Riga, 2019), 147–170.
20 State of Israel, *The 2014 Gaza Conflict: Factual and Legal Aspects* (Jerusalem, 2015), 73–97.
21 Gemunder Center for Defense and Strategy Hybrid Warfare Task Force, *Defending the Fence: Legal and Operational Challenges in Hamas-Israel Clashes, 2018-19* (Jewish Institute for National Security of America, Washington, DC, 2019).

militias on US forces and interests in the Middle East region'.[22] For its part, Iran relied on the same inherent right of self-defence to justify targeting a United States military facility located in Iraq on 8 January 2020 in response to what it condemned as the unlawful killing of Soleimani.[23] In both cases, the legality of one party's reaction hinges on the illegality of the other party's prior conduct.[24] Accordingly, the two legal arguments cannot be correct at the same time.[25] Regardless of their merits, these arguments thus illustrate the parallel process of legitimisation and delegitimisation at work.

Although law has always served as a strategic enabler and constraint in international relations in the manner just described, its reach and influence has evolved substantially in recent decades. Virtually all aspects of life in developed societies have become more densely regulated.[26] Similar processes have been at work at the international level, where the last three decades have witnessed the steady increase in both the volume and reach of international rules and the growing regulatory impact of international institutions, at least until more recently.[27] As a result, compliance with rules of law and questions of legal accountability have assumed greater importance in public affairs than ever before. The legality of foreign policy action comes under regular scrutiny, at least in Western nations, and the impact of law as a yardstick of governmental legitimacy has grown. This increased legalism is a source of considerable strength for liberal and democratic societies, but it also poses challenges and creates vulnerabilities.[28] With the advent of social media, legal debates are often reduced to battles of narratives and counter-narratives.[29] Legality has thus become a matter of strategic communication, encouraging instrumentalist approaches to the law and rendering it more and more overtly politicised.

The instrumental use of law is often described as 'lawfare'. This term was coined to refer to the use or misuse of the law 'as a substitute for traditional military means to achieve an operational objec-tive'.[30] Examples include the use of human shields to deter an adversary reluctant to incur civilian casualties from attacking a lawful military objective and thus render it immune from attack in contra-vention of the law of armed conflict. However, as the examples cited in this report illustrate, States and non-State actors employ the law not only to achieve military objectives during times of war, but also to attain broader strategic goals outside the context of active hostilities. For present purposes, it is therefore preferable to describe these competitive interactions as the instrumentalisation of law for strategic purposes, rather than as lawfare.

22 Letter dated 8 January 2020 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, 9 January 2020, S/2020/20.
23 Letter dated 8 January 2020 from the Permanent Representative of the Islamic Republic of Iran to the United Nations addressed to the Secretary-General and the President of the Security Council, 8 January 2020, S/2020/19.
24 The right of self-defence is available in response to an unlawful armed attack.
25 This is so because no right of self-defence can be claimed against a lawful act of self-defence, meaning that at least one claim must be wrong. Though this does not exclude the possibility that both are legally wrong. See Geoffrey S. Corn and Rachel VanLandingham, 'Lawful Self-Defense vs. Revenge Strikes: Scrutinizing Iran and U.S. Uses of Force under International Law', Just Security, 9 January 2020 (https://www.justsecurity.org/67970/lawful-self-defense-vs-revenge-strikes-scrutinizing-iran-and-u-s-uses-of-force-under-international-law/).
26 Generally, see Lars Chr Blichner and Anders Molander, 'Mapping Juridification' (2008) 14 *European Law Journal* 36. In greater detail, see Florian Pfeil, *Globale Verrechtlichung: Global Governance und die Konstitutionalisierung des internationalen Rechts* (Nomos, Baden-Baden, 2011).
27 For a classic study, see Judith Goldstein, et al., 'Introduction: Legalization and World Politics' (2000) 54 385.
28 This point was made eloquently by President Aharon Barak of the Supreme Court of Israel in *Public Committee Against Torture in Israel v. Israel and General Security Service*, Case No HCJ 5100/94, 6 September 1999, ILDC 2115 (IL 1999), 53(4) PD 817, (1999) Is LR 567, 6th September 1999, para. 39 ('This is the destiny of a democracy—it does not see all means as acceptable, and the ways of its enemies are not always open before it. A democracy must sometimes fight with one hand tied behind its back. Even so, a democracy has the upper hand. The rule of law and the liberty of an individual constitute important components in its understanding of security. At the end of the day, they strengthen its spirit and this strength allows it to overcome its difficulties').
29 See David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-first Century* (Basic Books, New York, 2017).
30 Charles J. Dunlap, Jr, 'Lawfare Today: A Perspective' (2008) 3 *Yale Journal of International Affairs* 146, 146.

Issues and indicators for trend monitoring

- Actors: who is using law as an instrument of strategic competition? In addition to States, which non-State actors are doing so? Which agencies of a hostile actor are involved in the strategic use of law and what role do they play?
- Tactics and methods: how are hostile actors using the law for strategic purposes? What recurrent patterns and what operating procedures may be identified? What do these reveal about the strategic intentions of the actor?
- Instruments and processes: what legal regimes, processes and institutions do hostile actors rely on? What do these reveal about the capabilities of a hostile actor?
- Impact and effects: how effective are hostile actors in achieving their strategic goals through the use of law?
- Trends to watch: how deliberate and adept are hostile actors in using the law to pursue their strategic objectives? Are they expanding their efforts? Are they allocating additional resources to this end?

Law as a hybrid threat

Given the utility of law as a strategic instrument, it should not come as a surprise to find that States and non-State actors employ legal arguments and processes as tools of hybrid influencing. Law is one of the domains in which hybrid competition takes place.[31]

Building on a recent attempt to conceptualise hybrid threats,[32] we may speak of the use of law as part of a hybrid campaign. This is the case when a hostile actor deliberately combines and synchronises action in the legal domain with activities in other spheres to target the systemic vulnerabilities of democratic societies with malign intent, typically using methods borrowed from the strategic toolbox of authoritarian regimes, revisionist powers and rogue States. It is useful to elaborate on certain elements of this conceptual model.

First, the use of law as an instrument of strategic competition is commonplace. Competition in the international arena through law is normal; it may even be seen as a design feature of international law.[33] Consequently, the fact that Russia's legislation banning 'undesirable' foreign organisations is motivated by political considerations is hardly remarkable.[34] After all, what law is not motivated by political considerations? What makes the ban stand out is not its pursuit of some political purpose, but that its use of the law for the *specific* political purpose of oppression.[35] Seen through the lens of liberal and democratic values, this *specific* purpose is objectionable.[36]

Whether the aim pursued by a particular legislative measure is acceptable is, ultimately, a matter of political judgement. Exercising such judgement is inescapable: what is acceptable to one government or society may well be unacceptable to another. This is why the conceptual approach outlined above requires the presence of 'malign intent'. This requirement focuses attention on situations in which one actor uses the law for a purpose or to an effect that is detrimental to another actor's interests in a way that transcends, due to the significance of the interests at stake or the severity of the adverse impact upon them, the boundaries of normal, albeit adversarial,[37] lawyering. What amounts to malign intent in this context is something for each affected party to decide. The notion merely serves as a heuristic device to distinguish routine legal competition from hybrid legal threats.

In this respect, it is illuminating to refer to the Counter-Terrorism and Border Security Act 2019 adopted by the United Kingdom Parliament in February 2019. The Act amends existing counter-terrorism legislation in response to a string of terrorist incidents and other attacks suffered by the United Kingdom, including the poisoning of Sergei and Yulia Skripal on 4 March 2018 in Salisbury.[38] Among other measures, the Act empowers law enforcement officers at British ports and borders to question, search and detain persons who engage in 'hostile activity'. For these purposes, 'hostile activity' means the commission, preparation or instigation of a 'hostile act' carried out for, or on behalf of, a State other than the United Kingdom or otherwise in the interests of a State other than the United Kingdom. A 'hostile act' is in turn defined as an act that threatens the national security or the economic well-being of the United Kingdom or

31 See Joint Research Centre and European Centre of Excellence for Countering Hybrid Threats, *The Landscape of Hybrid Threats: A Conceptual Model* (European Commission, Brussels, 2020), section 4.1.9., (non-public report).
32 Ibid., section 2.1.
33 Monica Hakimi, 'The Work of International Law' (2017) 58 *Harvard International Law Journal* 1.
34 See note 4.
35 Françoise Daucé, 'The Government and Human Rights Groups in Russia: Civilized Oppression?' (2014) 10 *Journal of Civil Society* 239.
36 See John C. Hamlett, 'The Constitutionality of Russia's Undesirable NGO Law' (2017) *UCLA Journal of International Law and Foreign Affairs* 246.
37 Robert Kagan defines adversarial legalism as characterised by 'formal legal contestation' and 'litigant activism', both prominent features of law in international affairs. See Robert A. Kagan, *Adversarial legalism: The American Way of Law* (Harvard University Press, Cambridge, Mass., 2001), 9. The dividing line between 'normal' adversarial and 'malign' lawyering is thus a matter of degree, rather than one of kind.
38 The Prime Minister (Mrs Theresa May), HC Deb, 14 March 2018, vol. 637, col. 856.

is an act of serious crime. While these definitions have been criticised as overly broad,[39] they underline that, in the present context, hostile or malign intent is a matter of political judgement based on the national interest.

Second, the preceding points do not imply that normative considerations are irrelevant. Exercising political judgement may be inescapable to determine whether a third party uses law with malign intent, but what counts as a normatively valid and compelling legal argument depends on legal, not political, criteria. States and other actors do engage in legal competition in formal settings, including before national and international courts and other judicial bodies. In 2013, for example, the Philippines instituted arbitration proceedings against China under the United Nations Convention on the Law of the Sea in relation to the South China Sea.[40] In formal venues and proceedings such as these, arguments normally succeed or fail on their legal persuasiveness, not their political appeal. Indeed, the arbitral award went against China. Countering hybrid legal threats therefore demands a high level of technical legal expertise.

Nevertheless, States also make spurious legal claims. In response to the United Kingdom's contention that Russia was responsible for poisoning Sergei and Yulia Skripal and that this act amounted to the use of force in contravention of Article 2(4) of the United Nations Charter,[41] Russia's Permanent Representative to the United Nations suggested that by accusing Russia in this manner, the United Kingdom itself had violated the prohibition against *threatening* the use of force set out in Article 2(4) of the Charter.[42] Threatening to use force would be unlawful in circumstances where the actual use of force itself would not be lawful[43]—but in the present case, nothing in the United Kingdom's statements can reasonably be construed as implying a threat to use force at all. Technical legal expertise is required to respond to legal claims that are tenable, but also to call out those that are blatantly not.

More generally, States committed to a rules-based international order must recognise that rules of law have an inherent value beyond their political utility. That value derives from the formality of law as an argumentative system and practice based on certain rules on what count as valid arguments. It is this feature that distinguishes legal from non-legal claims and law from mere politics. What this means, in practical terms, is that States with an interest in upholding a rules-based order ought to defend it against hybrid threats that undermine the rule of law not just when their strategic interests are implicated in a particular case, but also as a matter of principle. Many hybrid tactics, such as non-compliance, exploiting legal thresholds and grey areas, avoiding accountability and attribution, and making spurious legal claims,[44] are corrosive to the rule of law. Such tactics must be defused and hostile actors must be deterred from their repeated use. It also means that States committed to the rule of law must tread carefully to remain within the boundaries of international law or risk being accused of double standards.[45]

Third, States rely on law to achieve effects in other domains, just as they rely on non-legal measures to achieve effects in the legal domain. It is this combination that justifies describing law as a potential *hybrid* threat. How legal and non-legal effects may complement each other in a synergistic manner is illustrated by Chinese policy in the South China Sea.[46]

China has for some time argued that it enjoys sovereign rights over certain land features and

39 Robbie Stern, 'New U.K. Border Security Law: A Frightening Response to the Skripal Poisoning', Just Security, 20 March 2019 (https://www.justsecurity.org/63305/new-u-k-border-security-law-a-frightening-response-to-the-skripal-poisoning/).
40 Counter-Terrorism and Border Security Act 2019, Schedule 3, para 1.
41 Letter dated 13 March 2018 from the Chargé d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council, 13 March 2018, S/2018/218.
42 Security Council, 8203rd Meeting, 14 March 2018, S/PV.8203, 8.
43 *Legality of the Use by a State of Nuclear Weapons in Armed Conflict* (Advisory Opinion) (1996) ICJ Rep. 66, para. 47. See Nikolas Stürchler, *The Threat of Force in International Law* (Cambridge University Press, Cambridge, 2007).
44 See Parliamentary Assembly of the Council of Europe, Resolution 2217 (2018), Legal Challenges Related to Hybrid War and Human Rights, 26 April 2018, para. 5.
45 E.g. Statement by H.E. Mr. Sergey Lavrov, Minister of Foreign Affairs of the Russian Federation, at the 74th session of the UN General Assembly, New York, 27 September 2019 (https://www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/3822351).
46 Cf. Alessio Patalano, 'When Strategy is 'Hybrid' and not 'Grey': Reviewing Chinese Military and Constabulary Coercion at Sea' (2018) 31 *Pacific Review* 811.

their adjacent waters in the South China Sea.[47] This position is based on China's claim to have exercised control over these formations and waters throughout much of recorded history. China's claims are disputed by other States. The Chinese position was scrutinised in depth during the arbitral proceedings initiated by the Philippines, with the tribunal finding no evidence that China exercised exclusive control over the waters and resources concerned.[48] Nevertheless, China has taken a series of practical and legal measures to bolster its posture. It has maintained a continuous presence on various land formations in the South China Sea, carrying out extensive land reclamation or 'island-building' on seven reefs in the Spratly Islands.[49] In addition to providing China with strategic reach,[50] these activities transform maritime features which do not provide an entitlement to a territorial sea or exclusive economic zone under the United Nations Convention on the Law of the Sea into territorial formations over which China appears to claim sovereign entitlements.[51] Based on this self-created precedent, China now exploits the natural resources in these waters and denies other nations from accessing them, including by harassing and interfering with international maritime and airborne traffic.

Chinese legal and non-legal measures are thus mutually complementary. China claims historical rights to assert its authority in the South China Sea; creates *faits accomplis* on the basis of these legal claims to consolidate and expand them; and relies on a mix of military and paramilitary assets to deter other nations from challenging its authority and legal position *in situ*. The law supports operational effects and operations support legal effects.

Issues and indicators for trend monitoring

- Synchronisation: how do hostile actors combine action in the legal domain with activities in other spheres? In what way do legal activities complement their non-legal activities and objectives, and *vice versa*?
- Intent: what malign strategic objectives do hostile actors pursue through legal means and in the legal domain? How can their malign intent be identified and measured?
- Systemic vulnerabilities: what specific vulnerabilities are hostile actors targeting through the use of legal means? Is the law itself one of these vulnerabilities?
- Use and abuse of law: what normative criteria distinguish the legally permissible and legitimate use of law from its impermissible and illegitimate abuse? What, if anything, do such criteria contribute to identifying and measuring malign intent?
- Trends to watch: are hostile actors synchronising action in the legal domain with action in other areas in a more deliberate manner? Are they increasing their efforts and capabilities to pursue operational effects through legal means? Are they becoming more effective?

47 'Statement of the Government of the People's Republic of China on China's Territorial Sovereignty and Maritime Rights and Interests in the South China Sea' (2016) 15 *Chinese Journal of International Law* 903. See also Jianming Shen, 'China's Sovereignty over the South China Sea Islands: A Historical Perspective' (2002) 1 *Chinese Journal of International Law* 94.
48 *South China Sea Arbitration* (note 4), paras 263–272. For an overview, see Bernard H. Oxman, 'The South China Sea Arbitration Award' (2016) *University of Miami International and Comparative Law Review* 235.
49 Ibid., paras 852–890. See also Daniel Andreeff, 'Legal Implications of China's Land Reclamation Projects on the Spratly Islands' (2014) 47 *New York University Journal of International Law and Politics* 855.
50 Asia Maritime Transparency Initiative, 'Signaling Sovereignty: Chinese Patrols at Contested Reefs', 26 September 2019 (https://amti.csis.org/signaling-sovereignty-chinese-patrols-at-contested-reefs/; Asia Maritime Transparency Initiative, 'China Lands First Bomber on South China Sea Island', 18 May 2018 (https://amti.csis.org/china-lands-first-bomber-south-china-sea-island/).
51 *South China Sea Arbitration* (note 4), paras 1017–1018. See also Imogen Saunders, 'Artificial Islands and Territory in International Law' (2019) *Vanderbilt Journal of Transnational Law* 643.

Legal grey areas

Ambiguity and uncertainty are inherent features of every legal system. The meaning of legal texts is often obscure, competences may be ill-defined and novel situations are largely not foreseen by legislators. Rules of law do not interpret or apply themselves automatically in such situations. In fact, any act of interpretation or application of the law demands making decisions and choices. The outcome of some of these can be predicted with a degree of confidence, while the outcome of others cannot.

Although legal uncertainty is mostly seen as undesirable, it does confer some benefits. For example, ambiguity may produce a deterrent effect. Leaving some doubt in the minds of potential aggressors about the thresholds that trigger collective self-defence arrangements, such as those found in Article 5 of the North Atlantic Treaty, may cause adversaries to act more carefully.[52] However, while legal uncertainty and grey areas do have certain benefits, they also present tremendous opportunities to competitors for advancing their strategic interests. The regulation of cyberspace offers an example.

In a landmark agreement reached in 2013, States represented in the Group of Governmental Experts on advancing responsible State behaviour in cyberspace established by the United Nations General Assembly accepted that international law, including the United Nations Charter, is applicable in the cyber domain.[53] This fundamental principle has been affirmed more recently by the United Nations General Assembly and is supported by a broad international consensus.[54] However, it has proven more difficult to reach agreement on *how* the relevant rules should apply.[55] In line with its position that the existing rules for the most part are sufficient for regulating conduct in cyberspace, the United States has primarily focused its efforts on clarifying how, in its view, rules developed for an analogue world map onto the digital and cyber domain.[56] By contrast, China has taken the view that the existing rules of international law are inadequate and has therefore promoted the development of new norms.[57] This approach, coupled with China's insistence on cyber sovereignty and the right to develop its own domestic model of cyber regulation,[58] maximises China's ability to influence and shape the emerging regulatory framework of cyberspace and seeks to neutralise any competitive advantage that the United States and other Western nations may enjoy in this sphere.[59]

Besides norm entrepreneurship, legal grey areas also give hostile actors opportunities for more direct action. Generally speaking, States are not required to point to specific permissions to act on the international level. Provided their conduct is not prohibited by any applicable rules of international law, States may act freely by virtue of their sovereign status pursuant to what is known as the *Lotus* principle.[60] This has important implications

52 Ministry of Defence, *Deterrence: The Defence Contribution*, JDN 1/19 (Development, Concepts and Doctrine Centre, Shrivenham, 2019), 47.
53 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013, para. 19.
54 United Nations General Assembly Resolution 73/266, Advancing responsible State behaviour in cyberspace in the context of international security, 22 December 2018.
55 For an overview of the divergent positions, see Zhixiong Huang and Kubo Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches' (2017) 16 *Chinese Journal of International Law* 271.
56 See Brian J. Egan, United States Department of State Legal Advisor, Remarks on International Law and Stability in Cyberspace, Berkeley Law School, 10 November 2016 (https://2009-2017.state.gov/s/l/releases/remarks/264303.htm).
57 Ministry of Foreign Affairs and Cyberspace Administration of China, International Strategy of Cooperation on Cyberspace, 1 March 2017 (http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm). See Zhang Xinbao, 'China's Strategy for International Cooperation on Cyberspace' (2017) 16 *Chinese Journal of International Law* 377. See also Ma Xinmin, 'What Kind of Internet Order Do We Need?' (2015) 14 *Chinese Journal of International Law* 399.
58 See Remarks by H.E. Xi Jinping, President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference, Wuzhen, 16 December 2015 (https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml).
59 On Chinese norm entrepreneurship, see Congyan Cai, *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously* (Oxford University Press, New York, 2019), 150–152.
60 *S.S. Lotus (France v. Turkey)* (1927) PCIJ Series A, No 10, 18 ('International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free [...] Restrictions upon the independence of States cannot therefore be presumed').

in the information domain, for instance. While information and other influence operations undertaken by one State against another may amount to a *threat* of force prohibited by Article 2(4) of the United Nations Charter,[61] it is unlikely that such operations would amount to an *actual use* of force, unless they were to cause physical injury or damage. This is because Article 2(4) for the most part prohibits only the use of physical or kinetic force.[62] Hostile influence operations are therefore more likely to be caught by the principle of non-intervention, which prohibits interference that seeks to coerce the targeted State in 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.[63] However, two difficulties arise here. It is not settled what acts constitute prohibited coercion for the purposes of the non-intervention principle. Falsifying election records or sabotaging democratic processes is generally understood as qualifying as coercive intervention,[64] but whether spreading disinformation or leaking sensitive data with the aim of sowing discord and confusion does so too is open to debate.[65] Nor is it settled whether international law prohibits non-coercive interference that falls below the threshold of prohibited intervention.[66] The United Kingdom, for example, has taken the position that sovereignty has not given rise to a specific rule that prohibits such interference.[67] If this is correct, understanding where the threshold lies, on the one hand, between coercive intervention prohibited by the principle of non-intervention, and, on the other, interference left unregulated by international law assumes even greater significance. The grey area that results from this lack of legal certainty allows States conducting offensive influence operations to do so without normative constraints or the risk of suffering adverse legal consequences.

Operating on the boundaries of the law also makes it easier for hostile actors to get away with minor or incremental infractions of the rules. In November 2013, China established an Air Defence Identification Zone (ADIZ) over the East China Sea.[68] Although not expressly regulated by any international instrument, the establishment of such zones is generally understood to derive from, or at least be consistent with, a State's right to regulate the entry of aircraft engaged in international air navigation into its territory.[69] However, China's ADIZ applies to all aircraft entering the zone, whether or not they intend to enter Chinese national airspace, and is not limited to civil aircraft.[70] This is difficult to reconcile with the freedom of overflight enjoyed by other States.[71] China has also declared that its 'armed forces will adopt defensive emergency measures to respond to

61 Cf. The Judge Advocate General's Center and School, *Operational Law Handbook* (International and Operational Law Department, 17th edn, 2017), 135–141. Generally, see Anne Lagerwall and François Dubuisson, 'The Threat of the Use of Force and Ultimata', in Mark Weller (ed.) *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, Oxford, 2015) 911.
62 However, matters are complicated by the fact that the prohibition also extends to certain acts that are only indirectly or potentially destructive in their effect, such as military training and the provision of weapons. See *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)*, (Merits) (1986) ICJ Rep. 14, para. 228. It is not clear whether the provision of intelligence may also fall within this category. A further complication derives from the uncertainty as to whether interference with certain data, such as the deletion of software files, should be classed as non-kinetic or kinetic in nature. See Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 *Israel Law Review* 55 and Michael N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 *Israel Law Review* 81.
63 *Nicaragua Case* (note 62), para. 205.
64 Michael N. Schmitt, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' 19 *Chicago Journal of International Law* 30, 50.
65 For example, see Björnstjern Baade, 'Fake News and International Law' (2019) 29 *European Journal of International Law* 1357; Ido Kilovaty, 'Doxfare—Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information' (2018) 9 *Harvard National Security Journal* 146.
66 The point was acknowledged recently by Paul C. Ney, Jr., General Counsel of the United States Department of Defense, in his Remarks at U.S. Cyber Command Legal Conference, 2 March 2020 (https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/).
67 Attorney General Jeremy Wright QC MP, Cyber and International Law in the 21st Century, 23 May 2018 (https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century). The competing arguments are set out by Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 *AJIL Unbound* 207 and Michael N. Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 *Texas Law Review* 1639.
68 Statement by the Government of the People's Republic of China on Establishing the East China Sea Air Defense Identification Zone, 13 November 2013 (https://www.chinadaily.com.cn/china/2013-11/23/content_17126611.htm).
69 Cf. Article 11, Convention on International Civil Aviation, 7 December 1944, 15 UNTS 295. See Christopher M. Petras, 'The Law of Air Mobility – The International Legal Principles behind the U.S. Mobility Air Forces' Mission' (2010) *Air Force Law Review* 1, 63–64. See also Zoltan Papp, 'Air Defense Identification Zone (ADIZ) in the Light of Public International Law' (2015) *Pecs Journal of International and European Law* 28. But see Stefan A. Kaiser, 'The Legal Status of Air Defense Identification Zones: Tensions over the East China Sea' (2014) *Zeitschrift fur Luft- und Weltraumrecht* 527.
70 Announcement of the Aircraft Identification Rules for the East China Sea Air Defense Identification Zone of the People's Republic of China, 13 November 2013 (https://www.chinadaily.com.cn/china/2013-11/23/content_17126618.htm).
71 Articles 58 and 87, United Nations Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 3.

aircraft that do not cooperate in the identification or refuse to follow the instructions'.[72] This raises concerns of whether China intends to intercept non-compliant aircraft forcefully. Moreover, the area covered by the Chinese ADIZ overlaps with pre-existing ADIZs established by Japan and South Korea and extends into airspace over Socotra Rock and the Senkakus, both of which are the object of maritime disputes with Japan and South Korea, respectively. The unilateral declaration of the Chinese ADIZ was therefore escalatory in character.[73] The establishment of ADIZs has become an increasingly common international practice, but one that does not rest on an express treaty foundation and is not subject to a clear regulatory framework. This has created a legal grey area where China is able to assert its authority in a way that is not *per se* unlawful, but which diverges from established practice and pushes up against, and in certain aspects crosses, the relevant legal boundaries.[74]

Issues and indicators for trend monitoring

- Legal grey areas: what legal gaps, uncertainties and other weaknesses do hostile actors exploit and in what areas of law?
- Norm entrepreneurship: how do hostile actors seek to transform, adapt and exercise influence over existing legal regimes, processes, institutions and relationships to their own strategic advantage? What new regimes, processes, institutions and relationships do they seek to develop for these purposes?
- Incremental gains: how do hostile actors exploit salami-slicing tactics and create *faits accomplis* in the legal domain to achieve gradual strategic gains over time? How are such tactics identified?
- Trends to watch: what impact does the exploitation of legal grey areas by hostile actors have on the international legal system?
  How and in what way are hostile actors seeking to change the international legal *status quo*?
  What strategic gains do hostile actors achieve by exploiting legal grey areas, through norm entrepreneurship and by engaging in calculated violations of the law?

72 Announcement (note 70).
73 Raul Pedrozo, 'The Bull in the China Shop: Raising Tensions in the Asia-Pacific Region' (2014) 90 *International Law Studies* 66, 73–74.
74 See Roncevert Almond, 'Clearing the Air above the East China Sea: The Primary Elements of Aircraft Defense Identification Zones' (2015) 7 *Harvard National Security Journal* 126, 197; Jaemin Lee, 'China's Declaration of an Air Defense Identification Zone in the East China Sea: Implications for Public International Law', ASIL Insights, 19 August 2014 (https://www.asil.org/insights/volume/18/issue/17/china%E2%80%99s-declaration-air-defense-identification-zone-east-china-sea).

Legal fault lines and interfaces

In addition to taking advantage of legal grey areas, hostile actors exploit legal seams and interfaces, such as those that run between domestic law and international law, or between different national jurisdictions.

The Russian Government has repeatedly relied on the International Police Organisation (INTERPOL) notice system to pursue its political opponents.[75] The notice system enables national police authorities to share information with their foreign counterparts and to request their assistance, including in seeking the arrest of a person. INTERPOL is strictly forbidden from undertaking 'any intervention or activities of a political, military, religious or racial character'.[76] However, upholding this principle of political neutrality whilst screening politically motivated notices issued by its member States poses a real challenge.[77] As a result, it falls chiefly to the national authorities of a requested State to deal with politically motivated requests for cooperation. One of the most high-profile cases in this context is that of American-born British financier Bill Browder. Browder was instrumental in the adoption of the Magnitsky Act, a United States law that imposes sanctions on Russian officials implicated in the death of Russian tax advisor Sergei Magnitsky in a Moscow prison in 2009.[78] Between 2010 and 2013, the Russian authorities issued more than a dozen requests under the INTERPOL system for the extradition of Browder from the United Kingdom to face various charges in Russia. The Home Office rejected all of these notices on the basis that granting them was likely 'to prejudice the sovereignty, security, *ordre public*, or other essential interests of the United Kingdom'.[79] In May 2013, INTERPOL itself concluded that the case against Browder was of a predominantly political nature and deleted the information it held on him from all INTERPOL databases.[80] When only a few weeks later Russia issued yet another notice for Browder's arrest, INTERPOL took the unusual step of making a public statement declaring that 'INTERPOL cannot be used by the Russian Federation to seek the arrest of Mr William Browder'.[81] This has not deterred Russia. In May 2018, Browder was detained by police in Spain after Russia issued a renewed request for his arrest.[82]

More recently, the Russian authorities have initiated criminal proceedings against Lithuanian prosecutors, investigators and judges. The proceedings are an act of retaliation in response to the trial *in absentia* of former Soviet officers and officials on charges of war crimes and crimes against humanity for their role in the violent suppression of Lithuania's transition to independence in 1991. Concerns have been raised that Russia may misuse the INTERPOL system to seek the international arrest of the Lithuanian prosecutors and judges concerned.[83]

The case of the INTERPOL notice system demonstrates how authoritarian States may manipulate, with greater or lesser success, international norms and institutions to leverage the domestic legal processes of democratic societies against their political opponents. State authorities may use proxies to achieve the same effect, especially as this may afford them plausible deniability. Proceed-

75 David Satter, *Russia's Abuse of Interpol* (Henry Jackson Society, London, 2015).
76 Constitution of the International Criminal Police Organization-INTERPOL, 13 June 1956, I/CONS/GA/1956.
77 See Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe, Abusive Use of the Interpol System: The Need for More Stringent Legal Safeguards, Doc. 14277, 29 March 2017.
78 Global Magnitsky Human Rights Accountability Act, 22 USC §§ 2656 (2016).
79 *Dalnyaya Step LLC* [2017] EWHC 756 (Ch), para. 19.
80 David M. Herszenhorn, 'Interpol Rebuffs Russia in Its Hunt for a Kremlin Critic', *The New York Times*, 25 May 2013.
81 INTERPOL, 'INTERPOL cannot be used by the Russian Federation to seek the arrest of Mr William Browder', 26 July 2013 (https://www.interpol.int/en/News-and-Events/News/2013/INTERPOL-cannot-be-used-by-the-Russian-Federation-to-seek-the-arrest-of-Mr-William-Browder).
82 Ellen Barry and Raphael Minder, 'Bill Browder, a Putin Critic, Live-Tweets His Arrest in Spain' *The New York Times*, 30 May 2018.
83 European Parliament Resolution of 28 November 2019 on Recent Actions by the Russian Federation against Lithuanian Judges, Prosecutors and Investigators involved in Investigating the Tragic Events of 13 January 1991 in Vilnius, 2019/2938 (RSP).

ings initiated by private parties may also pursue broader strategic objectives, whether deliberately or inadvertently. For example, in 2012, a retired Russian police officer sanctioned under the Magnitsky Act for his alleged involvement in the murder of Sergei Magnitsky instituted libel proceedings against Bill Browder in the United Kingdom, taking issue with various accusations that Browder was said to have made against him.[84] Applying a balancing test, the High Court struck out the claim as an abuse of the process and/or under its inherent jurisdiction.[85] In a more recent case, a claimant originally from the Palestinian Territories, but resident in the Netherlands and holding Dutch nationality, launched civil proceedings before the Dutch courts against two senior Israeli military officers for their involvement in the alleged commission of a war crime during Operation Protective Edge in the Gaza Strip in 2014, requesting damages exceeding €500,000.[86] The Hague District Court found that the defendants enjoyed functional immunity from Dutch jurisdiction for their acts carried out in an official capacity and dismissed the claim. In a more recent case, four employees of the All-Russia State Television and Radio Broadcasting Company instituted proceedings against Lithuania before the European Court of Human Rights.[87] The applicants claimed that their expulsion from Lithuania and ban from reentering the country for one year violated their fundamental rights, including their freedom of expression. The European Court dismissed these claims, seeing no grounds to disagree with the national courts that the applicants behaved aggressively and provocatively at an official political event and that their expulsion was justified in the interests of national security.[88] While it would be a mistake to assume that all proceedings initiated by private parties in such circumstances must be abusive or undertaken to advance hostile State interests, it would be rash to dismiss the possibility that some of them might be or that they might otherwise complement a hybrid campaign.

In addition to exploiting legal interfaces for offensive purposes, States may rely on the fault lines and boundaries running between different legal systems in a more defensive manner, in particular to mitigate the impact that international and foreign norms may have on their domestic law.

In March 2015, a Russian subsidiary of the German manufacturing giant Siemens entered into a contract with Tekhnopromexport, a Russian company, for the manufacture, assembly and delivery of four gas turbines to Russia. Since European Union sanctions adopted in response to the annexation of Crimea prohibit the sale, supply, transfer and export of certain goods and technologies in the energy sector to any natural or legal person, entity or body in Crimea, or for the use in the Crimean peninsula or Sevastopol,[89] Siemens sought and received assurances that the turbines would not be transferred to Crimea or used exclusively to supply power to Crimea. Despite providing these assurances, Tekhnopromexport did in fact transport the four turbines to the Crimean peninsula for installation at power plants in Sevastopol and Simferopol. Siemens thereupon applied to the Moscow Arbitration Court to have the contract set aside as fraudulent and to recover the units.[90] Applying the Russian Civil Code, the Moscow Arbitration Court held that there was insufficient evidence to invalidate the contract based on fraud, misconception or deception. The Court also rejected the argument that Siemens was bound to comply with the export restrictions adopted by the European Union. According to the Court, accepting this argument would have amounted to a *de jure* application of the economic sanctions imposed by the European Union on the Russian Federation. This would

84 *Karpov v. Browder, Hermitage Capital Management Ltd, Hermitage Capital Management (UK) Ltd and Firestone* [2013] EWHC 3071 (QB).
85 However, it is worth noting that similar actions brought by the claimant, Pavel Karpov, against Bill Browder in Russia were dismissed by the Russian courts.
86 *Zarubin and Others v. Lithuania*, Application no. 69111/17, Decision, 26 November 2019.
87 Ibid., para. 56.
88 *Case C/09/554385/HA ZA 18/647*, Judgment of 29 January 2020, ECLI:NL:RBDHA:2020:667, Hague District Court (https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:667).
89 Article 2b, Council Regulation (EU) No 692/2014 of 23 June 2014 concerning Restrictive Measures in Response to the Illegal Annexation of Crimea and Sevastopol [2014] OJ L183/9, as amended by Council Regulation (EU) No 1351/2014 of 18 December 2014 [2014] OJ L365/46.
90 Решение Арбитражного суда г. Москвы от 17.01.2018 по делу N A40-191025/17-149-1807 [Decision of the Moscow Arbitration Court of 17 January 2018 in the case of N A40-191025/17-149-1807] (http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=MARB&n=1570213&dst=0&hash=0#08534216047054722).

be contrary to the public order of Russia, for it would undermine the sovereignty of the State. In any event, the Court pointed out that as a company incorporated under Russian law, Siemens' Russian subsidiary had no obligation to comply with foreign economic sanctions as a matter of Russian law. The Court thus dismissed the case.[91] The judgment illustrates how principles of public order and sovereignty enable a domestic legal system to insulate itself from the impact of measures adopted in foreign jurisdictions.

Domestic law can also serve as a shield against international law. Under the Russian Constitution of 1993,[92] rules of international law are accorded a prominent place within the Russian legal system. Pursuant to Article 15(4) of the Constitution, universally recognised principles and norms of international law as well as international agreements of the Russian Federation form an integral part of Russian law. Should a conflict between an international agreement and domestic law arise, Article 15(4) stipulates that the rules of the international agreement must be applied. However, this international law-friendly approach has come under increasing pressure. Ever since it acceded to the European Convention on Human Rights in 1998,[93] Russia has been on the receiving end of a growing number of individual applications under the Convention. By mid-2019, a total of 16,433 applications were pending against Russia.[94] Some of the cases are highly sensitive. In 2011, Russia lost an application brought by Yukos, an oil company stripped of its assets by the Kremlin as part of its efforts to curb the influence of Russia's oligarchs.[95] In July 2014, the European Court of Human Rights ordered Russia to pay an unprecedented amount of €1.87 billion in compensation to Yukos' shareholders.[96] The decision prompted a major backlash in Russia, leading a group of parliamentary deputies to request the Russian Constitutional Court to annul the domestic law directing the Russian authorities to comply with the judgments of the Strasbourg Court. While the Constitutional Court declined to annul the law in question, it held that Russia could refuse to execute a judgment of the European Court if its implementation was found to be incompatible with the Russian Constitution.[97] In 2015, Russia's parliament authorised the President and the Government to request the Constitutional Court to review the compatibility of Strasbourg judgments with the Constitution for these purposes.[98] The Constitutional Court subsequently found that the execution of the judgment in the *Yukos* case would be unconstitutional.[99]

91 The judgment was upheld on appeal. See Постановление Девятого арбитражного апелляционного суда от 10.04.2018 N 09АП-9815/2018 [Resolution of the Ninth Arbitration Court of Appeal of 10 April 2018, N 09АП-9815/2018] (http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=MARB009&n=1479773#06599149502436759); Постановление Арбитражного суда Московского округа от 27.06.2018 N Ф05-8233/2018 [Decision of the Arbitration Court of the Moscow District of 27 June 2018, N Ф05-8233/2018] (http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=AMS&n=296244#0088287818858599 04); and Определение Верховного Суда РФ от 29.10.2018 N 305-ЭС18-16459 [Decision of the Supreme Court of the Russian Federation of 29 October 2018, N 305-ES18-16459] (http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=558799&dst=0&hash=0#08837688466388444).
92 Constitution of the Russian Federation, 12 December 1993 (http://archive.government.ru/eng/gov/base/54.html).
93 Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1951, ETS No 5.
94 European Court of Human Rights, Press Country Profile: Russia (January 2020) (https://www.echr.coe.int/Documents/CP_Russia_ENG.pdf). However, thousands of these applications are likely to be found inadmissible and not progress to the merits.
95 *OAO Neftyanaya Kompaniya Yukos v. Russia* (Application No 14902/04), Judgment, 20 September 2011.
96 *OAO Neftyanaya Kompaniya Yukos v. Russia* (Application No 14902/04), Judgment (Just Satisfaction), 31 July 2014.
97 *On the Constitutionality of Provisions of Russian Domestic Law establishing the Obligation to Implement Judgments of the European Court of Human Rights*, Judgment No 21-P, ILDC 2455 (RU 2015), 14 July 2015. The judgment may be found at http://doc.ksrf.ru/decision/KSRFDecision201896.pdf. See Lauri Mälksoo, 'Russia's Constitutional Court Defies the European Court of Human Rights: Constitutional Court of the Russian Federation Judgment of 14 July 2015, No 21-П/2015' (2016) 12 *European Constitutional Law Review* 377.
98 These amendments are not compatible with Russia's obligations to abide by the final judgment of the European Court in any case to which it is a party pursuant to Article 46 of the European Convention on Human Rights. See Venice Commission, Council of Europe, Draft Final Opinion on the Amendments to the Federal Constitutional Law on the Constitutional Court, CDL(2016)018, 25 May 2016, para. 42. See also Kerttu Mager, 'Enforcing the Judgments of the ECtHR in Russia in Light of the Amendments to the Law on the Constitutional Court' (2016) 24 *Juridica International* 14.
99 *Ministry of Justice of the Russian Federation v. Shareholders of Oil Company 'YUKOS'*, Constitutional Proceedings, No 1-P / 2017, No 1-П/2017, ILDC 2648 (RU 2017), 19 January 2017. The judgment may be found at http://doc.ksrf.ru/decision/KSRFDecision258613.pdf. See Iryna Marchuk, 'Flexing Muscles (Yet Again): The Russian Constitutional Court's Defiance of the Authority of the ECtHR in the Yukos Case', EJIL:Talk, 13 February 2017 (https://www.ejiltalk.org/flexing-muscles-yet-again-the-russian-constitutional-courts-defiance-of-the-authority-of-the-ecthr-in-the-yukos-case/). This judgment follows on the heels of the earlier case of *On resolving the Matter of the Possibility of Implementing the Judgment of the European Court of Human Rights of 4 July 2013 in the Anchugov and Gladkov v. Russian Federation case in accordance with the Constitution of the Russian Federation*, Constitutional proceedings, No 12-P, ILDC 2590 (RU 2016), 19 April 2016. The judgment may be found at http://doc.ksrf.ru/decision/KSRFDecision230222.pdf. See Marina Aksenova, 'Anchugov and Gladkov is not Enforceable: the Russian Constitutional Court Opines in its First ECtHR Implementation Case', Opinio Juris, 25 April 2016 (http://opiniojuris.org/2016/04/25/anchugov-and-gladkov-is-not-enforceable-the-russian-constitutional-court-opines-in-its-first-ecthr-implementation-case/).

While these developments do not herald a comprehensive turn away from international law, they are symptomatic of a more assertive attitude that enlists notions of national sovereignty and 'constitutional identity' to mitigate the impact of unwelcome international norms in the Russian legal system.[100] Reinforcing this shift, President Putin recently proposed that the Russian Constitution should be revised to give effect to rules of international law, including decisions of international bodies, only insofar as they do not contradict the Constitution itself.[101] President Putin reportedly singled out the need to counter 'attempts to impose certain international laws on Russia from overseas' and 'unlawful' judgments of the European Court of Human Rights as the reasons for this proposal.[102] These concerns are not new. They reflect the rule of law objectives set out in Russia's Foreign Policy Doctrine of 2016, which include the objective of countering 'attempts by some States or groups of States to revise the generally accepted principles of international law' as enshrined in the United Nations Charter and countering 'politically motivated and self-interested attempts by some States to arbitrarily interpret the fundamental international legal norms and principles'.[103]

Legal fault lines may deepen existing vulnerabilities even when adversaries do not deliberately exploit the lack of legal interoperability. Take the example of cyber attacks. While the application of the rules governing the use of force in international relations to cyber attacks is not free from ambiguity, it is generally accepted that cyber operations may constitute an act of force or even amount to an armed attack triggering the right of individual or collective self-defence.[104] At their Wales Summit in September 2014, the Heads of State and Government of NATO's member States thus confirmed that a cyber attack could lead to the invocation of the mutual assistance obligation set out in Article 5 of the North Atlantic Treaty, though such a decision would be taken by the North Atlantic Council on a case-by-case basis.[105] Vulnerabilities may arise when such decisions intersect with other areas of law and sectors of society. For instance, insurers may make their own determination as to whether a cyber attack amounts to a 'war' for the purposes of insurance policies. Cyber operations designed to cause economic damage may thus lead to a fragmented legal response and cause further insecurity in the markets. In turn, this may create opportunities for State and non-State actors to exploit.

Issues and indicators for trend monitoring

- Legal seams and interfaces: what fault lines running between different legal regimes, jurisdictions and areas of the law do hostile actors exploit and how?
- Leveraging norms: which domestic legal regimes, processes and institutions of democratic societies are susceptible to being exploited by hostile actors? What international regimes and organisations are at risk of being subverted for hostile purposes?
- Shielding: what domestic legal instruments and other measures do hostile actors employ to minimise the impact of foreign norms and legal measures, including the impact of international rules applicable to them?
- Trends to watch: how deliberate and effective are hostile actors in targeting the domestic legal systems of democratic societies? What impact does competition in and through the legal domain have on international institutions and the international rule of law more generally? How effective are hostile actors in insulating themselves and their societies from external legal effects?

100 See Marina Aksenova and Iryna Marchuk, 'Reinventing or Rediscovering International Law? The Russian Constitutional Court's Uneasy Dialogue with the European Court of Human Rights' (2019) 16 *International Journal of Constitutional Law* 1322; Jeffrey Kahn, 'The Relationship between the European Court of Human Rights and the Constitutional Court of the Russian Federation: Conflicting Conceptions of Sovereignty in Strasbourg and St Petersburg' (2019) 30 *European Journal of International Law* 933.
101 Presidential Address to the Federal Assembly, 15 January 2020 (http://en.kremlin.ru/events/president/news/62582).
102 TASS, 'Putin notes ECHR sometimes makes unlawful decisions regarding Russia', 16 January 2020 (https://tass.com/politics/1109749).
103 Foreign Policy Concept of the Russian Federation approved by President of the Russian Federation Vladimir Putin on 30 November 2016, para. 26(b) (https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248).
104 See Michael N. Schmitt (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press, Cambridge, 2017), 328.
105 Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, NATO Press Release (2014) 120, para. 63 (https://www.nato.int/cps/en/natohq/official_texts_112964.htm).

Outlook and recommendations

There are few signs to suggest that geostrategic competition will abate in the near future. On the contrary, most indicators point in the direction of a more confrontational security environment. This has two implications for governments and societies committed to the ideal of a rules-based international order. First, sustained efforts must be made to uphold the international rule of law and to strengthen the norms, institutions and processes on which the international legal system depends. Second, if competition in the legal domain remains a prominent feature of the strategic landscape, then thought must be given to how to compete more effectively in this sphere.

Both steps — defending the international rule of law and competing more effectively — would benefit from adopting a resilience mindset. The notion of resilience has become popular in recent years as a conceptual tool for countering the challenges presented by the increasingly hybrid nature of the security environment. In the legal domain, resilience is concerned with the resistance of legal systems to disturbances and their capacity to adapt in response. Building on existing definitions of resilience in other disciplines, *legal resilience* may be defined as the capacity of a legal system to resist, recover from and adapt to internal and external disturbances while maintaining its key functions and features, and its capacity to contribute to the resilience of other natural or social systems.[106] This definition focuses on the capacity of legal systems to cope with disturbances and thus draws attention to the task of countering such disturbances more effectively. It also highlights that resilience in the legal domain has two aspects: the resilience of the legal system itself and the contribution that law makes to the resilience of other social and functional domains.

Adopting a legal resilience perspective helps to gain a better understanding of the legal vulnerabilities that hybrid threats present and exploit. Legal resilience also serves as a policy goal by encouraging States committed to a rules-based international order to strengthen the capacity of international norms, institutions and processes to withstand shocks and to use international law and their own domestic legal systems to reinforce the ability of other domains to cope with hybrid threats.

Converting these lessons into policy action involves several steps.

First, it is imperative to understand the legal operating environment. A wealth of information about the strategic use of law is available in the public sphere. However, to serve as a basis for policy, this data must be assessed more systematically and more comprehensively. Such analysis should focus on the following: legal actors, both friendly and hostile; the tactics and methods they employ to pursue their strategic interests in and through the legal domain; the instruments and processes they employ for these ends; the impact and effects they achieve in doing so; and the legal and societal vulnerabilities that they exploit and target.

Second, policy in the legal domain needs to be more strategic. Having mapped the legal operating environment, expressing support for a rules-based international order in the abstract is not sufficient. Democratic governments must identify core interests, set objectives, decide on means and methods, and allocate resources to take appropriate measures. One avenue for developing such a strategic approach is to undertake high-level, inter-departmental processes at the national and international level leading to the formulation of legal resilience strategies. Not unlike national security strategies, such documents could define the overall approach of a government or international organisation, serve as guidance for relevant stakeholders and provide a conceptual and practical framework for policy action.

106 Cf. Aurel Sari, 'Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats', forthcoming in (2020) 33 *Cambridge Review of International Affairs*.

Third, it is essential to retain a strong base of technical legal expertise and experience. China, for example, invests heavily into strengthening its capacity in the field of international law.[107] Tellingly, a decision adopted by the Central Committee of the Communist Party of China on 23 October 2014 aims for China to 'vigorously participate in the formulation of international norms […], strengthen our country's discourse power and influence in international legal affairs [and] use legal methods to safeguard our country's sovereignty, security and development interests.'[108] The 500-page critical study produced by the Chinese Society for International Law to refute the award delivered in the South China Sea Arbitration illustrates the trend.[109] Addressing the risks and the opportunities of this greater engagement with international law requires human capital.

Fourth, to prevail in an environment of enhanced legal competition, it is necessary to carefully rethink — and potentially recalibrate —the role of legal experts and legal advice in the policy process. Employing legal advisers and expertise in a chiefly passive role by setting clients' legal compliance as its core task is unlikely to generate an effective response to hybrid legal threats. Countering such threats demands a more proactive approach that anticipates adversaries' hostile instrumentalisation of the law and responds by employing law and legal arguments more deliberately for strategic effect. Adopting such an approach may require adjustments to current decision-making processes, doctrines and training.

Fifth, legal experts must master the vocabulary and understand the core tenets of colleagues working in neighbouring domains, and *vice versa*. Mapping legal vulnerabilities and responding to them in a more strategic manner requires collaboration between legal and non-legal experts based on ongoing dialogue between these different communities. A minimum of proficiency in each other's disciplinary language and outlook is indispensable. For example, in the information and cyber sphere, the application of existing rules is often unclear and there is a chronic, though inevitable, discrepancy between the speed of technological innovation and legal regulation. Addressing these problems effectively requires collaboration between lawyers literate in information technology and information experts willing to engage with the law.

Sixth, bearing in mind the close connection between legality and legitimacy emphasised throughout this report, particular attention must be paid to the link between law and strategic communication. If a substantial part of legal competition takes the form of competing narratives and counter-narratives, then it is essential to better understand the dynamics involved and their impact on different audiences.

Finally, international organisations and bodies have an important role to play in supporting States in their efforts to counter hybrid legal threats. As the examples of legal grey zones and legal interfaces reviewed above illustrate, most hybrid legal threats demand a multinational, multi-domain response. States should make effective use of the international organisations and process available to them to develop and coordinate such responses.

107 See Cai (note 59), 112–113; Chatham House, *Exploring Public International Law Issues with Chinese Scholars – Part 4* (Chatham House, London, 2018), 3–4.
108 Central Committee of the Chinese Communist Party, Decision concerning Some Major Questions in Comprehensively Moving Governing the Country According to the law Forward, 23 October 2014 (https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward/). See also Gu Zuxue, 'International Law as the Law of Domestic Governance: China's Propositions and Institutional Practice' (2017) 38 *Social Sciences in China* 157, 158.
109 Chinese Society of International Law, 'The South China Sea Arbitration Awards: A Critical Study' (2018) 17 *Chinese Journal of International Law* 207. For an assessment of the study, see Douglas Guilfoyle, 'A new twist in the South China Sea Arbitration: The Chinese Society of International Law's Critical Study', EJIL:Talk, 25 May 2018 (https://www.ejiltalk.org/a-new-twist-in-the-south-china-sea-arbitration-the-chinese-society-of-international-laws-critical-study/).

List of contributors

Aurel, Sari, Associate Professor of Public International Law, Exeter University, UK

Binder, Christina, Chair for International Law and International Human Rights, Bunderswehr University, Munich, Austria

Brux, Hanna, Counsellor for European Union Law, German Ministry of Defence, Germany

de Hoon, Marieke, Assistant Professor, Law Faculty, Vrije University, Amsterdam, Netherlands

Kleczkowska, Agata, Assistant Professor, Polish Academy of Science, Poland

Leonaité, Erika, Assistant Professor in International Law, Vilnius University, Lithuania

Magilton, Elsbeth, Excecutive Director of the Space, Cyber and Telecommunications law programs, University of Nebraska, USA

Miluna, Ieva, Government advisor and lecturer, Riga Graduate School of Law, Latvia

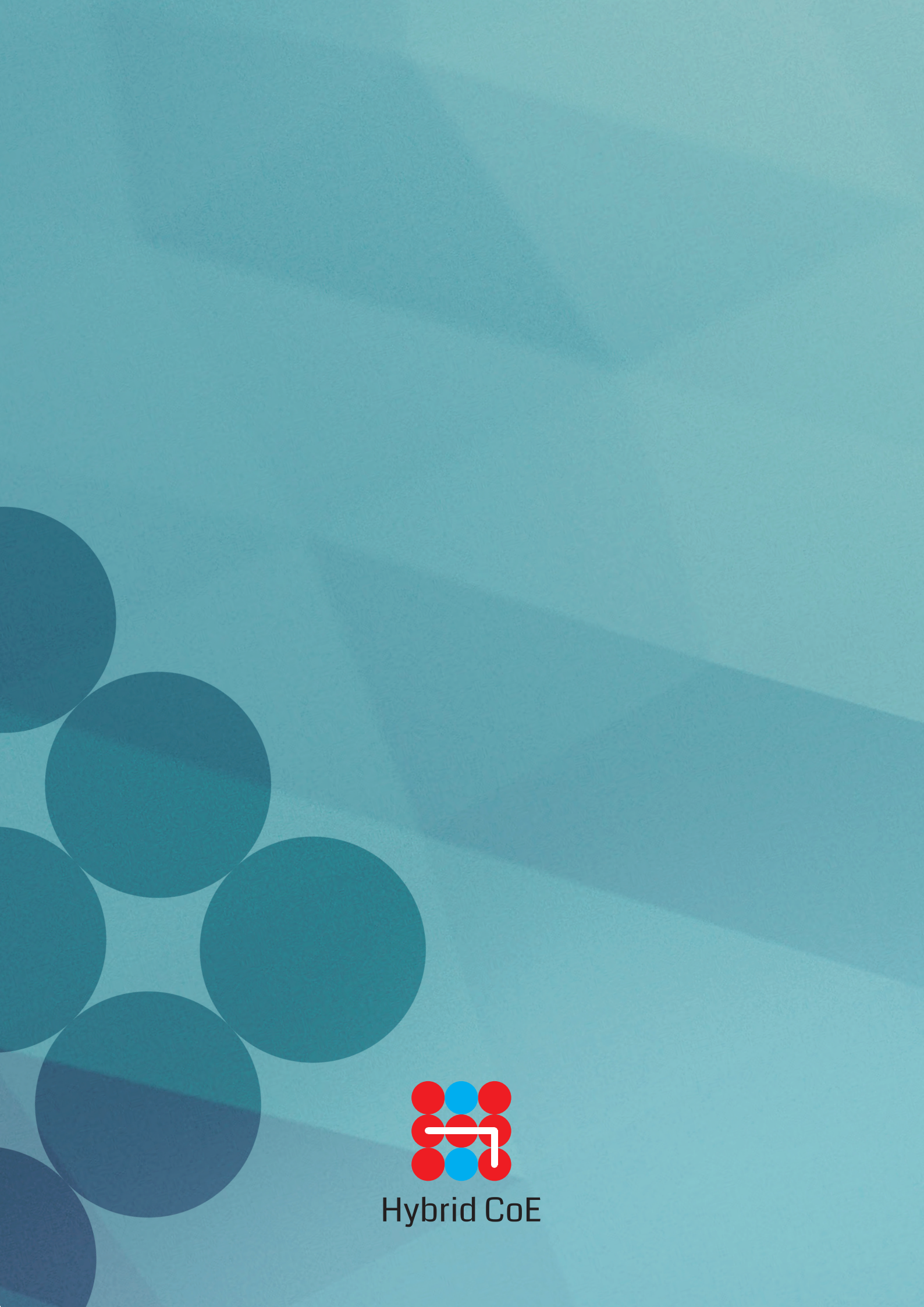
Orosan, Alina, Romania

Petman, Jarna, Senior Lecturer, Stockholm University, Finland

Schatz, Valentin, Research Associate, University of Hamburg, Germany

Suffia, Gabriele, Fellow research at the Information Society Law Center, University of Milan "C. Beccaria" Department, Italy

Ziccardi, Giovanni, Director of the Information Society Law Center, Professor, University of Milan "C. Beccaria" Department, Italy


Hybrid CoE