ARTICLES

SHAPING THE FUTURE OF EUROPE – SECOND PART
edited by Sandra Hummelbrunner, Lando Kirchmair, Benedikt Pirker, Anne-Carlijn Prickartz *and* Isabel Staudinger

EU LAW AGAINST HYBRID THREATS: A FIRST ASSESSMENT

LUIGI LONARDO*

TABLE OF CONTENTS: I. Introduction. – II. Disinformation. – II.1. Fake news. – II.2. Art. 114 TFEU: common foreign and security policy restrictive measures. – III. Foreign subsidies and investment. – III.1. "Hostile" subsidies and investment. – III.2. Art. 207 TFEU: the common commercial policy, the foreign direct investment screening regulation, trade defence instruments. – IV. Cybersecurity: "the dark side of the web". – IV.1. Cyber attacks to public targets. – IV.2. Arts 114, 215 and 352 TFEU: the EU Cybersecurity Act and the Critical Infrastructure Directive. – V. Border pressure. – V.1. Diverse threats for diverse borders. – V.2. Art. 77(2) TFEU: Area of Freedom, Security and Justice, and the Schengen Borders Code. Art. 82(2) and 83: EU criminal law, the Common Security and Defence Policy. – VI. Lawfare. – VI.1. Uses of law, abuses of law, and lawfare. – VI.2. Arts 2 and 3(5) TEU: can the EU engage in lawfare... in order to tackle lawfare? – VII. The future of security and defence law: emerging powers of the EU? – VIII. Conclusions.

ABSTRACT: The European Union defined hybrid threats as measures using diplomatic, military, economic and technological tactics to destabilise a political adversary. These threats are one of the emerging security challenges in Europe and have the potential to shape the future of the continent. It is EU policy that the primary responsibility for countering them lies with the Member States; and that NATO's mandate for the security of Europe makes it an important partner for the military and conventional deterrence aspects to tackle hybrid threats. This *Article* describes and discusses the legal tools available to the EU for deterring, mitigating or neutralising hybrid threats. The focus is on disinformation, hostile foreign subsidies and investment, cyber threats, border pressure, and lawfare. The EU seems, overall, legally well-equipped to counter the threats, thus positioning itself as the complementary and to a great extent autonomous ally of NATO in this domain. There is a distinctively supra-national dimension to virtually all of these threats, and this justifies that an EU competence arises. Hybrid threats cover such a broad array of issues that a single piece of legislation is neither feasible nor, probably, desirable; but if there were to be one, it would probably be based on art. 114 TFEU rather than on emergency clauses or on wholesale constitutional reforms. In any case, EU law will need to take into account that a close cooperation between the public and private sector is vital for countering hybrid threats.

* Lecturer in EU Law, University College Cork, luigi.lonardo@hotmail.com.

ISSN 2499-8249
doi: 10.15166/2499-8249/514

KEYWORDS: EU law – external relations – security and defence – hybrid threats – disinformation – competence.

I. INTRODUCTION

The notion of hybrid threats refers to compound techniques used to destabilise a political opponent. The European Union defines them as "multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by both state and non-state actors".[1]

This *Article* starts from one assumption: that hybrid threats to the EU have a degree of seriousness which makes them worthy of an effort to tackle them.[2] The assumption is widely shared by policymakers (EU institutions, and to a lesser and varied extent, national political leaders[3]), military commanders, and by researchers in this field. It appears to be justified in light of a precise Russian military doctrine[4] and of the long-standing Chinese political and military strategy of "three warfares" (public opinion warfare, media warfare, law warfare).[5] Moreover, the assumption is at the basis of the establishment of the European Centre of Excellence for Countering Hybrid Threats, inaugurated in 2017 with the support of both NATO and EU. The Covid-19 crisis has further fuelled the belief that hybrid threats pose a real danger.[6] Even if correct, the assump-

[1] Communication JOIN(2018) from the European Commission and the High Representative of the Union Foreign Affairs and Security Policy of 13 June 2018 on increasing resilience and bolstering capabilities to address hybrid threats. Other significant players give slightly different, but substantially equivalent definitions. They are recalled in D Fiott and R Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats' (2019) EUISS Chaillot Papers 4; scholarly debates over the definition and a new proposal are in M Wigell, 'Hybrid Interference as a Wedge Strategy: a Theory of External Interference in Liberal Democracy' (2019) International Affairs 255.

[2] The potential impact of each threat is best evaluated by relevant military, security, or political actors and falls outside the scope of this *Article*.

[3] See, for a useful overview, D Fiott, 'Uncharted Territory? Towards a Common Threat Analysis and a Strategic Compass for EU Security and Defence' (2020) EUISS Policy Brief 3.

[4] H Foy, 'Valery Gerasimov, the General with a Doctrine for Russia' (15 September 2017) Financial Times; and prior to that, the *maskirovka* (camouflage) was a doctrine integral to the Russian army.

[5] D Livermore, 'China's "Three Warfares" In Theory and Practice in the South China Sea' (25 March 2018) Georgetown Security Studies Review georgetownsecuritystudiesreview.org.

[6] Communication COM(2020) 605 final from the Commission to the European Parliament the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions of 24 July 2020 on the EU Security Union Strategy.

tion (and ensuing urgency in responding) does not imply that the EU's reaction is correct. Some of the measures taken to tackle the threats may prove counterproductive.[7]

Since the *Article* focusses on the EU, it is necessary to place its activity in perspective. Politically, the primary responsibility for countering hybrid threats lies with the Member States, and EU efforts are complementary in nature.[8] At international level, the security and defence of the European continent against such threats is largely ensured by the cooperation between the EU and NATO. Two joint declarations to this effect, of 2016[9] and 2018,[10] appear to divide the tasks pursuant to the respective mandates and capabilities of the organisations. While NATO is entrusted with conventional deterrence (military aspects), the EU is better equipped to deal with the civilian aspects. Given this political division of tasks, this *Article* is dedicated to answering the question of what legal tools the EU has for countering – deter, mitigate, or neutralise – hybrid threats.[11]

While the EU is now suggesting a single policy framework to face hybrid threats[12] (also with a view to adopt a Strategic Compass by 2022)[13] the legal framework is very fragmentary:[14] the label of hybrid threats is recent, it entered military strategy discus-

[7] See the example of actions against fake news, in section II.1. More generally, it is one of Tocqueville's lessons that half measures tend to work against their purposes, see A De Tocqueville, *The Ancien Régime and the French Revolution* (Cambridge University Press 2011) 139, and *ibid*., J Elster, 'Introduction' xxii.

[8] Council Conclusions of 10 December 2019 on complementary efforts to enhance resilience and counter hybrid threats.

[9] Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization of 8 July 2016 "The development of coordinated procedures through our respective playbooks will substantially contribute to implementing our efforts".

[10] Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, Brussels 2018 ("our partnership will continue to take place in the spirit of full mutual openness and in compliance with the decision-making autonomy and procedures of our respective organisations and without prejudice to the specific character of the security and defence policy of any of our members").

[11] It ought to be remembered nonetheless that the threats are hybrid also in the sense that they may couple civilian and military operations.

[12] See the Commission joint communications of 2016 and 2018. There is also a plethora of subject-specific policy documents, some of which are discussed in this *Article*.

[13] That is, an instrument contributing to forming a common strategic culture, see Council Conclusions of 17 June 2020, Security and Defence 3.

[14] There is no single piece of legislation containing EU tools to counter hybrid threats. EU competence may only arise when there is a cross-border element either to the threat or to the target thereof: but this is a sufficiently vast array of situations to warrant analysis. EU competence would be, most likely, to be based on one of the categories of the shared competences listed in art. 3(2) TFEU, or the Common Foreign and Security Policy and the Common Commercial Policy. Many measures have been or may be adopted in the context of harmonisation of the internal market, as discussed below for the cases of disinformation, IP theft, and privacy.

sion and political discourse,[15] and has not been "translated" into law yet. The EU policy framework and the institutional architecture have been object of excellent analyses.[16] Similarly, many legal profiles of hybrid threats have been dealt with in literature, but a comprehensive approach to EU regulatory response is still lacking.

This *Article* is structured around five hybrid threats: disinformation, hostile foreign subsidies and investment, cyberattacks, border pressure, and lawfare. In principle, the analysis could be structured by focussing on the target of the threat (infrastructures, borders, etc.); or the field to which the threat pertains (energy, internet, etc.); or on the EU competence engaged (energy law, migration law, Common Foreign and Security Policy, etc.). All these classifications, including the one this *Article* adopts, shed light to broadly overlapping aspects of the same phenomenon. The choice of structure of this *Article* is therefore justified in light of the definitionally hybrid nature of the threat, which is probably best captured by anchoring the analysis not to possible responses but to the threats themselves.

Each of the four sections of this *Article* is further divided into two parts. The first presents the threat; the second paints, with very broad strokes, the legal tools available to the EU to either deter, mitigate, or neutralise the threat.[17] In conclusion, in line with the theme of this special issue, the *Article* speculates on possible future developments of EU hybrid threats law and assesses possible constitutional implications.

II. Disinformation

II.1. Fake news

Disinformation is defined by the Commission as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[18] It is relatively cheap, can be carried out anonymously, and it may have far reaching-repercussions.[19] Disinformation has been especially linked to its potential to undermine the credibility of institutions, to "al-

[15] See A Missiroli, 'From Hybrid Warfare to "Cybrid" Campaigns: The New Normal?' NATO Defence College Policy Brief 19/19 1.

[16] *E.g.* D Fiott and R Parkes, 'Protecting Europe' cit. 4.

[17] The three actions structuring the final part of each section are taken verbatim from Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, art. 2(e), defining "protection".

[18] Communication COM(2018) 236 from the European Commission of 26 April 2018 on Tackling online disinformation: a European approach. This is the hybrid threat with the highest potential for philosophical speculation: what is false? And what counts as verification of falsehood? Why this almost metaphysical attachment to truth?

[19] The HR Borrell stated that disinformation in relation to Covid-19 can cost lives (Press conference by High Representative Josep Borrell Fontelles and Vice-President Věra Jourová on stepping up the response to disinformation around the coronavirus pandemic 10 June 2020).

ter political debate",[20] and has been perceived to have a distinctive target: liberal democracies,[21] attacked through undue influence over their key processes, such as elections, or at time of emergencies or acute uncertainty.[22] Since it is shared especially on social networks, it appears to affect prevalently younger generations. The threat has been identified by the EU (and NATO) as coming especially from Russia and ISIS – both of which had a dedicated apparatus for and a deliberate strategy of "disinformation" campaigns – and, in the context of Covid-19, also from China.[23] Its scale and effects might not be felt until it's too late: indeed, paradoxically, action taken to mitigate or neutralise a certain message identified as disinformation can produce the opposite effect, for example by lending it visibility.[24] The EU's strategic objective is to nullify the impact of disinformation coming from third countries, and its action has been based almost exclusively on non-legally binding instruments. The policy response has been to counter this threat with a strategic communication task force, established within the European External Action Service (EEAS).[25] This was followed by a Communication on tackling online disinformation (2018),[26] inspired by the principles of improving transparency, diversity, and credibility of information; and an Action Plan to step up efforts to counter disinformation (2018),[27] establishing a rapid alert system and urging private actors (online platforms) to implement the self-regulatory Code of Practice on Disinformation – applying to disinformation coming from third countries and from the EU itself.

II.2. Art. 114 TFEU: common foreign and security policy restrictive measures

The EU disposes of regulatory tools for the mitigation or neutralisation of disinformation (art. 114 TFEU), and "punishment" tools that may act as deterrent (restrictive measures adopted under the Common Foreign and Security Policy). This section considers them in turn. Legislative acts may be adopted by the EU to prohibit "fake news"

[20] D Fiott and R Parkes, 'Protecting Europe' cit. 34.

[21] M Wigell, 'Hybrid Interference as a Wedge Strategy' cit. 268.

[22] To describe the process in relation to Covid-19, the WHO and the EU have used the term "infodemic".

[23] See euvsdisinfo.eu.

[24] J Elster, *Sour Grapes: Studies in the Subversion of Rationality* (Cambridge University Press 2016) 46 discusses similar cases of "willing what cannot be willed".

[25] It was established following the European Council conclusions of March 2015 and an action plan submitted later that year by the High Representative for the Union's Foreign and Security Policy, in agreement with all the Member States. Two more tasks forces were established in 2017 for the Southern Neighbourhood and the Western Balkans.

[26] Communication COM(2018) 236 final cit.

[27] Communication JOIN(2018) 36 final of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions of 5 December 2018 on Action Plan against Disinformation.

and disinformation campaigns, arguably on the legal basis of art. 114 TFEU. That article provides a residual competence for the EU to approximate "provisions [...] in Member States which have as their object the establishment and functioning of the internal market". As such, it is "the central Treaty provision for harmonizing the laws of EU MS",[28] and as mentioned below other important instruments for the regulation of online content have been adopted on the same legal basis.

Such an EU measure to tackle disinformation would be enacted for the purposes of avoiding that illegal content be in circulation on platforms such as Facebook, Twitter, Instagram, who are hosting providers;[29] and avoiding that the disinformation creates undue distortions in the internal market. This is perhaps not the most appropriate option, in policy terms (for disinformation may do much more than simply causing trouble to a sector of the market), but it appears to be the most solid legal basis. The specificity of the damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extension. In addition, there exists the need to ensure that national authorities do not lose the mutual confidence which they should have in one another: this led the legislature of the EU to adopt the e-commerce directive[30] on the basis of art. 114,[31] or legislation on the IT society,[32] the proposed regulation against terrorist content online,[33] and the same rationale would apply for the legislation against fake news. Even though each Member State may seek the annulment of the act, legislation adopted pursuant to art. 114 TFEU tends to be confirmed by the Court of Justice of the European Union, which has been generally deferential to the choice of EU institutions when judicial challenges have risen. This measure would have the significant disadvantage of not being able to tackle effectively disinformation coming directly from third countries: EU law adopted on the basis of art. 114 TFEU would most likely apply to *external* threats if and only if there is an *internal* cross-border element, *i.e.* if at least two Member States are involved. So in *Baltic Media Alliance*, content produced in Russia and broadcasted in Lithuania was subject to EU law because the Court was satisfied that there was a

[28] M Kellerbauer, 'Article 114 TFEU' in M Kellerbauer, M Klamer and J Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019) 1236.

[29] The main social media platforms provide a service for the purposes of art. 1(1)(b) of the Directive 2015/1535/EU of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. They are service providers even when they are not liable for the content, as detailed in case C-18/18 *Eva Glawischnig-Piesczek v Facebook* ECLI:EU:C:2019:821 para. 22 discussed below.

[30] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[31] Art. 95 of the Treaty on the European Community, as it then was. We know this from recital 52 of the Directive.

[32] Directive 2015/1535/EU cit.

[33] Proposal COM(2018) 640 of 20 September 2018 of the Commission for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.

cross-border element: namely, the content was provided by a company established in the UK (at that time, an EU Member State) and this triggered the application of the audiovisual services directive.[34] If EU law were binding outside EU territory, it would give rise to the kind of conceptual legal difficulty that other instruments such as the e-commerce directive (see discussion below) are encountering – namely, making EU law binding in third countries. Another challenge would lie in the centralised determination of the content to be considered illegal. As of now, not all disinformation consists of statements that are unlawful (an example of "fake news" which is already unlawful is the one amounting to consumer fraud or constituting hate speech). The Commission would need to show that EU legislation defining what counts as illegal content respects the principle of subsidiarity, but admittedly leaving the choice to Member States would not meaningfully improve the current legislation (for under the e-commerce directive, Member States courts are already empowered to order the removal of illegal content). As any restriction to freedom of speech, whatever definition the EU legislature might adopt, must be proportionate, respect the essence of that right, and meet objectives of general interests (art. 52(1) of the EU Charter of Fundamental Rights).[35]

Another possible legal basis is the chapter of the TEU concerning Common Foreign and Security Policy (CFSP). Punitive measures cannot concern criminal law, for lack of EU competence, but may result in the imposition of restrictive measures under CFSP. The procedural requirements are stricter than the previous option, their scope narrower, and they would risk an uncertain outcome. Restrictive measures thus conceived would involve third-country natural or legal persons (either by targeting them directly or by prohibiting EU nationals from contracting with them). A case in point is that of Ms Bamba,[36] an Ivorian entrepreneur subject to restrictive measures because of her responsibility for publishing a newspaper that incited to hatred, violence, and disinformation campaigns on the 2010 presidential election in Ivory Coast. It is one of the few cases of restrictive measures adopted to tackle disinformation, but the campaign was only indirectly related to EU's security and defence. On that occasion, the Council targeted disinformation in order to safeguard democracy in a third country – but it is not to be excluded that it might do the same to shield the EU itself from this external threat.

[34] Case C-622/17 *Baltic Media Alliance* ECLI:EU:C:20119:566 para. 56.

[35] A Renda, 'The Legal Framework to Address "fake news": Possible Policy Actions at the EU level' (2018 European Parliament – Policy Department for Economic, Scientific and Quality of Life Policies).

[36] Case C-417/11 *Council v Bamba* ECLI:EU:C:2012:718.

III. Foreign subsidies and investment

III.1. "Hostile" subsidies and investment

The EU is committed to being open to foreign investment,[37] but measures adopted by third countries "appear to have an increasingly negative effect on competition in the internal market".[38] In a nutshell, the problem arises because, as the Commission's White Paper on foreign subsidies puts it, "EU State aid rules help to preserve a level playing field in the internal market among undertakings with regard to subsidies provided by EU Member States. However, there are no such rules for subsidies that non-EU authorities grant to undertakings operating in the internal market. This situation may include circumstances where the benefitting undertakings are owned or ultimately controlled by a non-EU company or a foreign government".[39] The grant of foreign subsidies may be driven, in some cases, "by a third country's strategic objective to establish a strong presence in the EU, or to promote an acquisition and later to transfer technologies to other production sites possibly outside the EU".[40] In addition, analysts have proposed to consider foreign investment in critical infrastructures as part of hybrid threats,[41] because of their potential to influence heavily the political behaviour of the host country's population.

In particular, China's ventures in Central, Eastern and Southern Europe have recently assumed proportions that aroused worry in Western Europe's political circles.[42] The same happened for China's investments in the EU's immediate neighbourhood. China's Belt and Road initiative has manifested itself in EU territory through bilateral international agreements (memoranda of understanding) signed between China and European countries (the so-called 16+1 initiative, which includes 12 EU Member States). As the 2019 EU strategy toward China states, those Chinese investments have "frequently neglect socioeconomic and financial sustainability and may result in high-level indebtedness and transfer of control over strategic assets and resources".[43] The competitiveness of European companies is further undermined by the fact that foreign companies may have access to subsidies, state-backed loans, export credits at preferential terms, and,

[37] It is, arguably, a constitutional commitment: art. 21(2)(e) TEU.

[38] Editorial, 'Protecting the EU's Internal Market in Times of Pandemic and Growing Trade Disputes: Some Reflections about the Challenges Posed by Foreign Subsidies' (2020) CMLRev 1366.

[39] European Commission, 'White Paper on levelling the playing field as regards foreign subsidies' Communication COM(2020) 253 final 6.

[40] Editorial, 'Protecting the EU's Internal Market in Times of Pandemic and Growing Trade Disputes' cit. 1366.

[41] M Demertzis and GB Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (2019) Bruegel Policy Contribution.

[42] J de Kok, 'Towards a European Framework for Foreign Investment Reviews' (2019) ELR 24.

[43] Communication COM(2019) 5 final from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament, the European Council and the Council of 12 March 2019 on EU-China – A strategic outlook.

outside the EU, to different labour market conditions. This is especially concerning for strategic industries (in the energy, transport, and, in the context of Covid-19, healthcare sector).[44] In this domain, deterrence may not be feasible, whereas a mitigation, if not complete neutralisation of whatever threat investment may pose, ought to be possible. The EU rules on investment, albeit not aimed specifically at tackling this situation, might ensure that the final choices over China's policy in central and eastern Europe belong to the EU legislature. This evinces perhaps an optimistic vision of the international order as based on rules and compliance with international agreements, an optimism on which there is bound to be political disagreement.

III.2. Art. 207 TFEU: the common commercial policy, the foreign direct investment screening regulation, trade defence instruments

Under EU law, investment is only partially caught by the Common Commercial Policy. The Court held that foreign direct investment falls within EU exclusive competence, regulated in the Common Commercial Policy (art. 207 TFEU),[45] whereas it is shared competence between the Member States and the EU in its non-direct forms such as portfolio investment, and in matters concerning investor-states dispute settlements.[46] EU investment policy is not only contained in EU agreements – sometimes split in separate agreements covering trade (exclusive competence) and investment protection agreements (shared competence)[47] – but also in a Regulation[48] detailing rules for the application of the hundreds of agreements between individual Member States and third countries. The above shows that the regulation of investment is a complex mosaic in which the EU and Member States' competence is intertwined. However, this does not mean that a Member State can unilaterally contract with a third country on this matter: rules on pre-emption (art. 3(2) TEU) apply so that, for example, Greece or Latvia are pre-empted from concluding a bilateral agreement with China or Russia if the subject mat-

[44] Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (2020/C 99 I/01).

[45] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, for example, was adopted on the basis of this article.

[46] Opinion 2/15, *Free Trade Agreement with Singapore* ECLI:EU:C:2016:992.

[47] Such is the case of the Agreement with Singapore and with Vietnam. Council Decision (EU) 2018/1599 of 15 October 2018 on the signing, on behalf of the European Union, of the Free Trade Agreement between the European Union and the Republic of Singapore and Council Decision (EU) 2019/1121 of 25 June 2019 on the signing, on behalf of the EU, of the Free Trade Agreement between the EU and the Socialist Republic of Viet Nam.

[48] Regulation (EU) 1219/2012 of the European Parliament and of the Council of 12 December 2012 establishing transitional arrangements for bilateral investment agreements between Member States and third countries.

ter of that agreement falls in a field already occupied by EU law (it would be a case of so-called supervening exclusivity of EU competence).[49] At the same time, EU free trade agreements usually contain national security clauses, which allow each party to derogate from rules or chapters of the agreement if it is to protect essential state interests.[50] These clauses may be activated, in mixed agreements, by Member States or by the EU to protect key sectors, such as essential industries, from hostile investments that might otherwise be allowed by the agreement in question. While the EU itself could rely on these clauses,[51] it is likely that Member States – who have competence in matters of national security – will be the first to invoke such exceptions.

The main legal instrument adopted by the EU in relation to hostile investments is the Foreign Direct Investment (FDI) screening regulation,[52] which has as legal basis art. 207(2) TFEU. The FDI screening regulation leaves the responsibility for screening FDI to Member States, who can review it on the grounds of security or public order and take measures to address specific risks. Similarly, under art. 65 TFEU, Member States may restrict the free movement of capital from third countries on the ground of public policy or public security. Crucially, the FDI screening regulation ultimately empowers Member States: it leaves them discretion on whether to screen FDI, but if they choose to do so, the regulation provides for a mechanism of co-ordination and provides for partial harmonisation.[53] In the light of Covid-19, the Commission has urged all Member States to set up a screening mechanism.[54] In addition, the EU can tackle foreign subsidies through so called "trade defence instruments". Part of these, countervailing measures are essentially anti-subsidies proceedings. The World Trade Organisation allows the adoption of countervailing measures in the "Agreement on Subsidies and Countervailing Measures" contained in Annex 1A of the WTO Agreement, to which EU international agreements usually refer.[55] The legal basis under EU law, adopted on the basis of art. 207(2) TFEU, is the Regulation on protection against subsidised imports.[56] Measures on

[49] On which see *e.g.* M Chamon, 'Implied Exclusive Powers in the ECJ'S Post-Lisbon Jurisprudence: The Continued Development of the ERTA Doctrine' (2018) CMLRev 1101.

[50] By way of example, the Free Trade Agreement with Singapore contains such a clause allowing derogations from rules on public procurement (art. 9(3)(1)); the Free Trade Agreement with Canada has the same for public procurement (art. 19(3)(1)(b)) and an additional all-encompassing clause related to essential security interests (art. 28(6)).

[51] Albeit not in the context of investment, in 2014 the EU took action as allowed under art. 99(1) of the Partnership and Cooperation agreement with Russia in light of the tension in Ukraine.

[52] Regulation 2019/452 cit.

[53] J Snell, 'Editorial: EU Foreign Direct Investment Screening: Europe Qui Protège?' (2019) ELR 138.

[54] Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (FDI Screening Regulation) (2020/C 99 I/01).

[55] *E.g.* arts 5-11 EU-Japan FTA; art. 3(1) EU-Vietnam FTA.

[56] Regulation (EU) 1037/2016 of the European Parliament and of the Council of 8 June 2016 on protection against subsidised imports from countries not members of the European Union.

anti-dumping and anti-subsidy matters applicable following a WTO Dispute settlement body report are contained in a further Regulation.[57] There are, nonetheless, important differences between the regime for foreign subsidies under WTO and EU law, with the important consequence that "it cannot be excluded that under one regime something is found to be a subsidy or aid whilst under the other it is not".[58]

IV. Cybersecurity: "the dark side of the web"

IV.1. Cyber-attacks to public targets

Usually, the use of the term cybersecurity "relates to four major societal threats – crime, cyberwar, cyber terrorism and espionage".[59]

Even a cursory mention of the potential *public* targets of criminal, terrorist, or war-like cyber-attacks renders the idea of the complexity of the issues involved, for which the treatment is here bound to be purely schematic:[60] critical infrastructures such as harbours, airports, or pipelines; industrial or civilian complexes (such as powerplants or hospitals); not to mention banks, military headquarters, and ministries. The digitalisation of human activities lends strong support to the fear of those who imagine apocalyptic scenarios in which the enemy gets possession, through a cyber-attack, of the adversary's military capabilities. Intellectual property theft was listed by the High Representative as a form of hybrid threat in a 2019 declaration. When it assumes the form of espionage through hacking, trade secret theft, or file sharing, it is considered a national security threat in the United States.[61] What these attacks have in common is the potential damage, if not downright paralysis, of core state functions. In that case, if state functions are affected, *ius ad bellum* profiles become relevant, in so far as it is NATO policy that a cyber-attack against a member might open the door to the alliance's response pursuant to art. 5 of the NATO Charter.

[57] Regulation (EU) 476/2015 of the European Parliament and of the Council of 11 March 2015 on the measures that the Union may take following a report adopted by the WTO Dispute Settlement Body concerning anti-dumping and anti-subsidy matters.

[58] Editorial, 'Protecting the EU's Internal Market in Times of Pandemic and Growing Trade Disputes: Some Reflections About the Challenges Posed by Foreign Subsidies' (2020) CMLRev 1377 for a discussion of these differences.

[59] E Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security' (2014) European Journal of Risk Regulation 47.

[60] See the special issue of the European Foreign Affairs Review, 2019, whence the Pink Floyd-sounding phrase is borrowed: A Missiroli, 'The Dark Side of the Web: Cyber as a Threat' (2019) European Foreign Affairs Review 135.

[61] D Halbert, 'Intellectual Property Theft and National Security: Agendas and Assumptions' (2016) The Information Society 256.

IV.2. Arts 114, 215 and 352 TFEU: the EU Cybersecurity Act and the Critical Infrastructure Directive

EU law countering cyber-attacks is predicated on three main instruments: the EU Cybersecurity Act (adopted on a legal basis of art. 114 TFEU),[62] the cyber-attacks sanctions framework regulation (based on art. 215 TFEU),[63] – both were adopted as part of the "Cyberdiplomacy toolbox"[64] – and the Critical Infrastructures Directive ("CID", based on art. 352 TFEU). This section considers them in turn, before considering other instruments relevant to cybersecurity. Overall, these EU measures aim to "build resilience, fight cybercrime, build cyberdefence, develop industrial and technical resources and elaborate a diplomatic strategy for cyberspace".[65]

The Cybersecurity Act defines cyber threat as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons".[66] In extreme synthesis, that Act increases significantly the mandate, the powers, and the resources of the European Union Agency for Cybersecurity (ENISA). It allows for the opportunity to develop a common response system between EU institutions, and entrusts ENISA with coordinating and supporting it as well as the Member States, both in terms of prevention and of response. The sanctions framework regulation applies to cyber-attack (including potential ones) provided that they meet a minimum threshold of having "significant" effect (by reasons of the criteria set out therein),[67] against the EU and/or its Member States.[68] The framework regulation allowed for the adoption, in July 2020, of the EU's first sanctions against cyber-attacks. The individuals and entities targeted were allegedly involved in an attempted cyber-attack against the Organisation for the Prohibition of Chemical Weapons, in Cloud Hopper, in WannaCry and NotPetya. The last three are among the most devastating cyber-attacks in history: they affected public services and critical infrastructures, had a far-reaching geographical spread, and the estimated damages amount to

[62] Regulation (EU) 881/2019 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act).

[63] Council Regulation (EU) 796/2019 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[64] Communication JOIN (2017) 450 of the European Commission and the High Representative of 13 September 2017 on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

[65] RA Wessel, 'European Law and Cyber Space' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) (on file with this author).

[66] Art. 2(8) of the Cybersecurity Act cit.

[67] In art. 2: scope, scale and impact or severity of the disruption, number of Member States or people affected, the economic benefit gained by the perpetrator etc.

[68] Art. 1 of the Council Regulation (EU) 796/2019 cit.

several billions of dollars.[69] The restrictive measures present an important issue bound to result in litigation before (EU) courts: the grounds for being targeted are contained in a short statement (the statement of reasons), but in light of the difficulty in attributing the cyber-attacks a court will face a very delicate choice, between deferring to the Council's choice (as it usually happens for restrictive measures)[70] or scrutinising it in light of the complex technical assessment needed.

When it comes to the CID, EU law identifies critical infrastructures as *physical* assets or systems located in Member States which are essential for the maintenance of vital societal functions (art. 2(a) CID).[71] It imposes on Member States obligations to conduct threat assessments (art. 7 CID), and most importantly lays down a common approach for the security of European critical infrastructures (those whose disruption would affect at least two Member States). The "common approach", as opposed to a centralised procedure, leaves discretion to Member States on the extent to which they wish to involve the Commission. It also sets common standards for infrastructures protection. *Digital* networks are, of course, possible targets of cyber-attacks. The EU adopted, in 2013, its first Cybersecurity strategy, and later a directive on network security.[72] The current discussion on 5G technology, with its risks and potentials, has an EU dimension: the Commission recommendation of March 2019 on cybersecurity 5G networks[73] follows the European Council's call for a concerted approach to this technology.

Intellectual property theft is particularly disruptive of competition – and cannot be confirmed until it is too late (that is, when a similar or identical product has appeared on another market). The target of this threat are most commonly private companies, and this elevates the need to private-public dialogue to an existential requirement, if the threat may be to public security. Under EU law, intellectual property crime may target industrial property and copyrighted material. As part of the digital single market strategy, the Commission adopted a series of recommendations to sustain small and medium enterprises in their fight against IP theft, in the context of the IP rights directive.[74] Within Europol, the Intellectual Property Crime Coordinated Coalition fights these crimes by giving operational and technical support to competent authorities, as well as harmonising and standardising legal instruments to counter IP crime. The latter function is particularly relevant for the purposes of this discussion.

[69] See *e.g.* KS Nash, S Castellanos and A Janofsky, 'One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs' (27 June 2018) Wall Street Journal www.wsj.com.

[70] See *e.g.* case C-72/15 *Rosneft* ECLI:EU:C:2017:236 para. 113.

[71] Directive 2008/114/EC of 8 December 2008 of the European Critical Infrastructures and the Assessment of the Need to Improve their Protection ('CID') on the Identification and Designation.

[72] Directive 2016/1148/EU of 6 July 2018 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union.

[73] Commission Recommendation COM(2019) 2335 on Cybersecurity of 5G networks of 26 March 2019.

[74] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

The EU has in place a robust legal framework for the protection of personal data.[75] EU law on data protection and online services is a muscular tool that allows prevention against data breaches and protects EU citizens even outside the territory of the EU. This extra-territorial application of EU law, as mentioned, has raised important legal issues that prove divisive among EU lawyers. In the case of the e-commerce directive, the Court has recently had occasion to pronounce over the reach of the protection granted by such legislative instrument. In *Glawischnig-Piesczek v Facebook*,[76] an Austrian politician was object of a Facebook comment which, under Austrian law, was considered illegal content. Austrian courts asked the ECJ whether EU law allows them to order Facebook to remove worldwide statements with identical wording and/or having equivalent content to the illegal one. The Court held that Facebook is a host provider for the purposes of the e-commerce directive even if it is not liable for the content. This is a very important point, as it entails the application of EU internal market rules to content hosted[77] by social media platforms (regardless of the author), provided that there is a link with EU law (*i.e*. the service provider is established in the EU, the recipient is an EU citizen, or the service is offered across Member States).[78] The Court also found that the host provider may be ordered to remove not only the illegal content, but also "information with an equivalent meaning" – provided that the order specifies with sufficient clarity what ought to be removed, so that it does not result in the host having to carry out an independent assessment.[79] Even though the Court is keen on stating that the host will exclusively have recourse to automated tools for locating and removing the content, some have expressed scepticism as to the technological feasibility of this task.[80] Finally, the Court found that the Courts of Member States may issue injunctions which produce worldwide effects, because there is no relevant limitation in the e-commerce directive. The finding of the Court strengthens the power and the scope of application of EU's legal response to hybrid threats targeting individuals (in the case under discussion, a politician), in so far as it expanded the substantive and geographical reach of the protection afforded.

[75] On this as well as on criminal measures adopted by the EU to combat cyber-crime see RA Wessel, 'European Law and Cyber Space' cit.

[76] *Eva Glawischnig-Piesczek v Facebook* cit.

[77] It will be recalled that hosting is a service pursuant to the definitions of the e-commerce directive and of Directive 2015/1535.

[78] *Eva Glawischnig-Piesczek v Facebook* cit. para. 22.

[79] *Ibid*. para. 46.

[80] P Cavaliere, 'AG Opinion on C-18/18: Towards Private Regulation of Speech Worldwide' (28 June 2019) European Law Blog europeanlawblog.eu.

V. Border pressure

V.1. Diverse threats for diverse borders

Borders are traditionally the place where skirmishes and confrontation first happens. Fiott and Parkes provided an excellent overview of the situations faced alongside the thousands of kilometres the EU shares with third countries, by sea or land.[81] The issues range from smuggling of people, drugs, and even garbage, to military provocation. It ought to be recalled that by their very nature, hybrid threats tend to be combined, so that border pressure can be exercised jointly with disinformation campaigns etc.

A necessary if artificial distinction ought to be drawn between the Eastern border and the Southern one. Some of the pressure from Russia is exercised directly by that State, hence the cause of the threat originates in the EU's neighbourhood. Some of the pressure against the Southern borders (Spain, Italy, Greece and the Balkans) does not originate directly from the neighbouring countries, but so to speak further away. The migratory flows from Syria and South-Saharan Africa and routed, respectively, through the Maghreb or Turkey are examples of a pressure whose genesis is not in the EU's immediate neighbourhood but which may be used, for example by Turkey, as leverage in negotiations with the EU.

V.2. Art. 77(2) TFEU: Area of Freedom, Security and Justice, and the Schengen Borders Code. Art. 82(2) and 83: EU criminal law, the Common Security and Defence Policy

In addition to a general migration and asylum policy, EU competence consists of rules for the management of Schengen borders (which is also most of EU external borders), now set out in the Schengen Borders Code,[82] through the independent agency Frontex and an integrated information system.[83] Frontex cooperates with national authorities for the purposes of border control and surveillance.

The EU has also adopted criminal law instruments for tackling border issues, based on the broad powers conferred to it under arts 82 and 83 TFEU. Reference shall be made to the directive on human trafficking,[84] and drug trafficking.[85] The legal basis of art. 83(1) TFEU in particular appears to be bestow quite a broad power to the EU, in so

[81] D Fiott and R Parkes, 'Protecting Europe' cit.

[82] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

[83] So-called SIS II, Regulation 1987/2006.

[84] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

[85] Council Framework Decision 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking.

far as it allows the adoption of measures to criminalise offences "in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis" (among which the article lists "border threats" such as human or drug trafficking, money laundering). The powers are broad because, on a literal reading of art. 83(1) TFEU, the EU may criminalise offences without a cross-border dimension, as long as they fall in one of the "areas of particularly serious crime" foreseen by said article.[86] Similarly broad powers are invested by art. 83(2) TFEU, under which the EU may adopt directives "if the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures". As mentioned later, these provisions lend themselves to a functional interpretation and are likely to result in an expansion of EU activity.

Complementarily to that, the EU has used instruments adopted pursuant to the Common Security and Defence Policy (CSDP) for patrolling the Mediterranean Sea,[87] such as the launch of the military operation EUNAVFOR MED in 2015.[88] The complementarity between the AFSJ and the CSDP derives from the fact that the latter is meant to be deployed outside the EU, at least if one heeds to the letter of art. 42(1) TEU.[89] CSDP military operations could also helpful for border surveillance and processing of irregular migrants, in support of Frontex.[90] What happens at the border, however, is only part of the story: as it is well-known, there are remote causes for migratory flows. These can be tackled and perhaps mitigated by the EU development policy and perhaps CSDP. In addition, civilian missions and military operations have been deployed for the purposes of contributing, directly or indirectly through capacity building of local forces, to a decrease in the amount of people who reach EU borders. An example of the former is EUCAP Sahel Niger, of the latter EUTM Mali.[91]

[86] But see, *contra*, I Wieczorek, *The Legitimacy of EU Criminal Law: Hart Studies in European Criminal Law* (Hart 2020) 114.

[87] On which see G Butler, 'EU Foreign Policy and Other EU External Relations in Times of Crisis: Forcing the Law to Overlap?' in E Kuzelewska, A Weatherburn and D Kloza (eds), *Irregular Migration as a Challenge for Democracy* (Intersentia 2018).

[88] Council Decision (CFSP) 2015/972 of 22 June 2015 launching the European Union military operation in the southern Central Mediterranean.

[89] "The Common Security and Defence Policy shall be an integral part of the CFSP [...] the Union may use them on missions outside the Union [...]". In this sense, see also S Biscop and J Rehrl, *Migration – How CSDP can support* (Publication of the Federal Ministry of Defence and Sports of the Republic of Austria 2016) 11.

[90] *Ibid*. 12.

[91] First approved through Council Decision (CFSP) 2013/34 of 17 January 2013 on a European Union military mission to contribute to the training of the Malian Armed Forces.

If the link between the eradication of poverty or security on one hand, and on the other hand reduction of migration is accepted, then the EU has tools to mitigate the remote causes of migratory flows which result in pressure on borders.

VI. Lawfare

VI.1. Uses of law, abuses of law, and lawfare

There is, finally, a sense in which law itself can be used by adversaries to exert pressure: law can be, in and of itself, a hybrid threat (not simply a tool or vehicle thereof). The proposition that law may be used for political aims is trivially true, but about what some analysts in the Euro-Atlantic area worry is, more or less explicitly, that the EU has too many rules, and that, paradoxically, the legal system becomes a cumbersome apparatus from which opponents can benefit.[92] The comparison is, once more, with China and Russia. These countries appear less encumbered by legal constraints,[93] or are perceived to engage in obstructionist, unprejudiced, or downright cynical use of law.[94] NATO's standpoint on confrontational "legal operations" concerns explicitly the latter. Authors have identified, for example, that "Russia's activities in the Arctic provide several good examples of manipulating the Rules Based International Order".[95] For instance, in 2015 Russia appealed to the UN for the recognition of a large portion of the Arctic Sea as part of Russia's Exclusive Economic Zone, thus purporting to act in compliance with public international law.[96] Those authors speculate that this claim was not made in good faith.

In addition to that, there is lawfare, can be defined as the "use [of] communication and informational media to propel certain legal concepts and interpretations into the public mindset that will help achieve strategic objectives".[97]

[92] On which see in general A Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats' (2019) Harvard National Security Journal 442-443.

[93] For the difficulties that this give rise to for the rule-of-law based EU, see the reflections in S Blockmans, 'Why Europe Should Harden Its Soft Power To Lawfare' (2020) CEPS in Brief www.ceps.eu.

[94] For example, using law for the purposes of achieving aims other than those for which the rules were originally conceived. Concrete cases are discussed in M Voyger, 'Russian Lawfare – Russia's Weaponisation of International and Domestic Law: Implications for the Region and Policy Recommendations' (2018) Journal of Baltic Security 38.

[95] B Seguin, 'The Use of Legal Operations in a Context of Hybrid Threats and Strategic Competition' (13 March 2020) Lawfire sites.duke.edu.

[96] *Ibid*.

[97] AB Munoz Mosquera and SDOV Bachmann, 'Lawfare in Hybrid Wars, The 21st Century Warfare' (2016) Journal of International Humanitarian Legal Studies 63.

VI.2. Arts 2 and 3(5) TEU: can the EU engage in lawfare... in order to tackle lawfare?

Since the rule of law is one of the fundamental values of the EU (art. 2 TEU), and, in its relations with the rest of the world, the EU shall contribute to "the strict observance and the development of international law, including respect for the principles of the United Nations Charter" (art. 3(5) TEU), it is inconceivable to envisage that the EU would develop an express policy commending cynical uses of law.[98] Paradoxically, the requirement to adhere to pre-established and democratically decided rules may be perceived as a vulnerability. Adversaries might exploit the difficulty in reaching consensus and the need to stick to procedures. From this perspective, the mutual defence clauses may invite opponents to act below their threshold,[99] or slightly above just to "test" if there is a reaction. However, the rule of law is a fundamental value common to the organisation of power, both public and private, in the Euro-Atlantic area. Its constitutional importance for the EU can hardly be set aside, perhaps not even in highly exceptional and most unusual circumstances requiring urgent action, lest the EU lose its nature and a new legal order be created. There are nonetheless areas in which the EU may have recourse to "lawful, though unfriendly, measures of international intercourse".[100] For once, the EU has engaged in what may be construed as lawfare, according to NATO's definition recalled above, in so far as it has set up the Strategic Communications task forces to counter disinformation, as recalled in section II.1 above. In addition, the EU has the power to adopt restrictive measures whose design is political in nature, *i.e*. subtracted from judicial control, even though it has to comply with human rights and procedural requirements. Finally, the EU has autonomous defence clauses which may be used as deterrent, and those are object of extensive analysis elsewhere.[101]

In any case, the uses of law for international relations are not limited to external competences. As Mills has correctly noted, "internal action by the EU has external effects, which should be viewed not merely as incidental but also as potentially instruments of external policy".[102] Mills referred to the developments of private international law, regulated "internally" at EU level and with repercussions for EU's external position:

[98] International law (*e.g*. art. 17 of the European Convention of Human Rights, art. 300 of the United Nations Convention on the Law of the Sea States), as well as the EU Charter of Fundamental Rights (art. 54), prohibit abuse of right.

[99] A Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties' cit. 444, referring to the classic TC Schelling, *Arms and Influence* (Yale University Press 2008) 35 ff.

[100] The citation is from A Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties' cit. 442.

[101] *Ibid*.

[102] A Mills, 'Private International Law and EU External Relations: Think Local Act Global, or Think Global Act Local?' (2016) ICLQ 541. Similarly, PG Andrade, 'EU External Competences in the Field of Migration: How to Act Externally When Thinking Internally' (2016) CMLRev 157.

for example, when the EU uses private international law "as a means of projecting policies extraterritorially by limiting access to EU recognition unless a foreign law or judgment complies with certain standards".[103] The same logic ought apply to EU law countering hybrid threats.

VII. The future of security and defence law: emerging powers of the EU?

A single legal instrument or a coherent legal framework is, at this stage, inexistent. This is because of the very nature of the danger, which is meant, by design, to escape detection and clear categorisation. There are two ways in which the EU might nonetheless conceive and implement a unitary legal response: through "horizontal" emergency provisions or through more or less explicit constitutional amendments.

Regardless of the specific policy area of Union action, recourse might be had to "horizontal" emergency provisions. The fundamental Treaties empower the EU (arts 66, 78(3) and 122 TFEU), its Member States (art. 42(7) TEU[104] and art. 65 TFEU), or a mixture of both (art. 222 TFEU)[105] to take action in emergency situations. For their breadth of scope, arts 222 TFEU and 42(7) TEU might seem appropriate for the task – whereas art. 78(3) TFEU, which refers to "an emergency situation characterised by a sudden inflow of nationals of third countries", is apt in the case of this border pressure. There are, however, two interrelated issues. The first is the very scope of those clauses. Do hybrid threats fall, by virtue of their subject matter, under the definition of either art. 222 TFEU or 42(7) TEU? Arguably, none of the threats identified above constitute, in and of themselves, an "armed aggression" for the purposes of art. 42(7) TEU; whereas damages to infrastructure may amount to "natural or man-made disaster" under art. 222 TFEU, or, if they affect product supply, art. 122 TFEU. The second is a policy argument concerning those definitions: an explicit indication of the threshold which would trigger the clauses under EU law may constitute an invitation to the adversaries. As it is often the case with "redlines", it may amount to an invitation for opponents to either act below that threshold (ie, causing disturbance without necessarily triggering a response), or to provoke the EU by carrying out an attack precisely to test the Union's response.

Alternatively, one might observe how recent event-driven developments of EU law have resulted in implicit constitutional amendments, later endorsed by the Court. The EU's response to the economic and financial crisis of the past decade displayed constitutional ingenuity that at times, if not systematically, stretched the letter of the Treaties

[103] A Mills, 'Private International Law and EU External Relations' cit. 543.

[104] P Koutrakos, 'The Role of Law in Common Security and Defence Policy: Functions, Limitations and Perceptions' (2011) European Foreign Policy: Legal And Political Perspectives 237 ff.

[105] C Hillion and S Blockmans, 'Europe's Self-defence: Tous Pour Un et Un Pour Tous?' (2015) CEPS Commentary.

and of EU's attributed competence. The pervasive reform of "constitutional redesign" that took place through the setup of Banking Union,[106] and especially the management of public finances outside the Treaties (*e.g*. with the European Stability Mechanism), may be considered to be *de facto* constitutional amendments. In that context, an economic and political rationale guided the reforms. In the name of effectiveness and expediency, the functions of the EU have expanded. It is interesting to speculate whether something similar could happen for hybrid threats. The security rationale might lead the EU to exercise, in practice, powers which go beyond what the Treaties appear to provide, at least if taken literally.[107] There are three reasons why certain EU actions in this domain might amount to an implicit constitutional amendment. The first is the express dictum of art. 4(2) TEU, according to which, as recalled, internal security is the sole responsibility of the Member States. The second is that it might encroach on NATO commitments for part of EU Member States, or on traditional neutrality for others,[108] something which (art. 42(2) TEU) appears to forbid. Additionally, the security threat might be tackled by EU Member States outside the framework of EU Treaties, for example through bilateral agreements. Examples of these, in the domain of defence, are the European intervention initiative (an agreement between eight Member States and the UK creating the pre-conditions for coordination of military operations[109]) or the Aachen Treaty (an international treaty between France and Germany on military cooperation).[110] The third is that if art. 83(2) TFEU were to be interpreted broadly, the recognition of implied powers in the area of criminal law may amount to a recognition of an EU (exclusive) competence in (part of) this field. Yet, it is not unconceivable that EU political institutions – backed by the Court – will find emerging powers or envisage some form of constitutional engineering to justify comprehensive EU action, if the threats reached a sufficient degree of seriousness. There is a distinctively EU dimension – and thus an EU interest – to virtually all of the threats discussed in this *Article*. There is shared awareness of this, at national and Union level. The 2016 Global Strategy makes this clear: "[n]one of our countries has the strength nor the resources to address these threats and seize the opportunities of our time alone".[111] Further, as mentioned, at least in the case of the areas of crimes of art. 83(1) TFEU a cross-border dimension needs not be established, as it is presumed in the list drawn by that article. With few exceptions,

[106] T Tridimas, 'General Report' (2016) Processes of the XXVII FIDE Report 87.

[107] See, for a similar argument in the field of cybersecurity, RA Wessel, 'European Law and Cyber Space' cit.

[108] As discussed in A Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties' cit.

[109] Letter of intent of 25 June 2018 between the Defence ministers of Belgium, Denmark, Estonia, France, Germany, the Netherlands, Portugal, Spain, and the UK.

[110] Treaty on Franco-German Cooperation and Integration of 22 January 2019.

[111] High Representative, 'Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy' (June 2016) 3.

Member States have little capabilities and overall an underdeveloped legal framework, at national level, for tackling hybrid threats.[112] As far as intelligence and counter-intelligence is concerned, it is worth restating here that many EU Member States are heavily reliant on cooperation within NATO.

In a sense, there was a meta-rationale of security[113] in the case of economic reforms as much as there would be if the response to hybrid threats led to constitutional changes: the underlying idea in both cases is the elevation of a threat to EU's activity to an existential issue, whereby EU inaction is considered tantamount to a complete failure of the integration project. Similar to this, if not precisely this, seems to be the understanding of the CJEU, which Takis Tridimas has called "the existentialist conception of EU competence".[114] Such existential understanding has manifested itself also at times not of emergency: in the interpretation of the internal market harmonisation clause (art. 114 TFEU),[115] or in the protection of the "essence of rights" in the context of EU citizenship.[116] The CJEU has been actively involved in approving an expansive understanding of EU competence, and this might not change in the context of hybrid threats.

VIII. Conclusions

Legal and regulatory tools equip the EU to counter the hybrid threats mentioned in this *Article*, thus positioning the Union as the complementary and to a great extent autonomous allied of NATO in this domain. While the threats themselves are very broad, so are EU competences. The three understandings of the word "countering" – deterring, mitigating, and neutralising – are helpful to paint a picture of the potential of the EU's legal framework, even though it should be clear that there will always be "unknown unknowns",[117] so that complete neutralisation is chimerical.

To tackle disinformation, the EU may avail itself of the general clause of art. 114 TFEU to pass legislation regulating news that might adversely affect the internal market. However, it would be more difficult to find EU competence to regulate disinformation coming directly from third countries and targeting individual Member States. On investment, art. 207 TFEU on the Common Commercial Policy affords the EU with competence to regulate to a capillary extent trade and investment with China. Even in the absence of a Free Trade Agreement, EU law often pre-empts bilateral agreements between third countries and EU

[112] G Gressel, 'Protecting Europe Against Hybrid Threats' (2019) European Council for Foreign Relations.

[113] To borrow the expression from M Fichera, *The Foundations of the EU as a Polity* (Edward Elgar 2018) 1.

[114] T Tridimas, 'The ECJ and the National Courts: Dialogue, Cooperation, and Instability' in D Chalmers and A Arnull (eds), *The Oxford Handbook of European Union Law* (Oxford University Press 2015).

[115] *Ibid*.

[116] Case C-34/09 *Zambrano* ECLI:EU:C:2011:124.

[117] To borrow the concept from Donald Rumsfeld's speech at the US Department of Defence News Briefing of 12 February 2002: there will always be facts or threats that are ignored until... they materialise.

Member States on this subject. EU has capabilities to increase the resilience of Member States against cyber-attacks to critical infrastructures, to individuals, or to intellectual property, as the instruments adopted on the basis of arts 114, 215 and 352 TFEU show. This is done not by deterring third countries with threats of retaliation, but by strengthening EU-level networks of cooperation. The EU has a special interest in the contribution to border management, as witnessed by the emphasis in policy documents of the Commission. It is also competent to establish rules for both Schengen and non-Schengen borders (within the Area of Freedom Security and Justice, or through criminal law, arts 82 and 83 TFEU). Finally, as far as lawfare is concerned, the EU can adopt perfectly lawful yet unfriendly measures (such as sanctions) to deter or mitigate other threats (such as disinformation). The EU has proved successful in mitigating many threats. It could be particularly strong in the deterrence dimension, in its non-military aspects: earlier detection and prevention of the threats is, probably, the best deterrence.

Hybrid threats cover such a broad array of issues that a single legal instrument is neither feasible nor, probably, desirable. If it were to be developed, it would most likely be built on a set of legal bases, spanning from art. 114 TFEU on the approximation of the internal market, to the Common Commercial Policy,[118] rather than on emergency clauses or on wholesale constitutional reforms.

In any case, close cooperation with the private sector is vital, and this is the most likely long-term impact of any legal framework that may be developed to challenge hybrid threats. The threats are not only tackled, but also put by companies or individuals whose affiliation with a sovereign state is always more or less plausibly deniable.[119] The European Commission is aware of this necessary development. If the notion of hybrid threats is destined to be fashionable in the next decades, it might inaugurate an era, if not of privatization of security and defence, at least of diffusion into the private sector of the core public function.

[118] The Common Security and Defence Policy does not seem to offer legal instruments material to this discussion, but rather policy tools.

[119] G Gressel, 'Protecting Europe Against Hybrid Threats' cit.