University of Groningen

From strategic communication to sanctions

Giumelli, Francesco; Cusumano, Eugenio; Besana, Matteo

Published in:
A Civil-Military Response to Hybrid Threats

DOI:
[10.1007/978-3-319-60798-6_8](https://doi.org/10.1007/978-3-319-60798-6_8)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2017

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

Giumelli, F., Cusumano, E., & Besana, M. (2017). From strategic communication to sanctions: The European Union's approach to hybrid threats. In *A Civil-Military Response to Hybrid Threats* (pp. 145-167). Springer International Publishing. https://doi.org/10.1007/978-3-319-60798-6_8

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats

*Francesco Giumelli, Eugenio Cusumano,
and Matteo Besana*

As epitomised by the 2016 Communication outlining a 'Joint Framework on Countering Hybrid Threats', the European Union (EU) is increasingly involved in tackling destabilisation challenges ranging from disinformation to energy disruptions and cyberattacks. This chapter examines EU response to hybrid threats by looking at two types of policy instruments. The first one, the fight against disinformation, is a 'soft' type of response that the EU has increasingly adopted since 2015 as an answer to misinformation campaigns that have targeted it by a variety of actors, including Russia and the self-proclaimed Islamic State.

F. Giumelli (✉)

Department of International Relations and International Organization (IRIO),
University of Groningen, Groningen, The Netherlands

E. Cusumano

University of Leiden, Leiden, The Netherlands

M. Besana

CCOE, The Hague, The Netherlands

The second one is a more traditional, ‘hard’ form of action, namely, the planning and implementation of sanctions and restrictive measures. Not only are strategic communication and sanctions key to countering hybrid threats. As this chapter illustrates, both policy instruments require especially close cooperation across military and civilian public actors and between the public and the private sector. Hence, strategic communications and sanctions are crucial cases in the study of EU responses to hybrid threats and the importance of a comprehensive approach in effectively countering them.

The chapter is divided as follows. The first section examines the EU approach to hybrid threats, examining relevant documents and discussions about the appropriate role of the EU in countering challenges ranging from the proliferation of weapons of mass destruction to cyberattacks, energy disruptions and information warfare. The second section looks at the risks that disinformation poses to the EU’s democratic processes and the strategic communication policies that have been formulated in response. The third section introduces EU sanctions, focusing on the use of this policy instrument to counter hybrid threats and enhance the resilience of the EU and its partner countries. The conclusions draw on this body of evidence to provide some recommendations on countering misinformation and improving the effectiveness of EU restrictive measures, stressing the importance of a comprehensive approach to both strategic communication and the design and implementation of sanctions.

1 THE EU APPROACH TO HYBRID THREATS

The EU embraced the concept of hybrid threats much later than NATO, which already introduced the notion of hybridity in its doctrine and policy in 2010. Hybridity entered EU jargon only in April 2016, when the High Representative (HR) for the Common Security and Defence Policy (CSDP) issued a ‘Joint Framework on countering hybrid threats’. The Joint Framework was followed by an operational protocol between member states, the Commission and the HR for Foreign Affairs and Security Policy. Hybrid threats are also repeatedly mentioned in the June 2016 Global Strategy, where they are identified as a key challenge to the security of the EU. This section will briefly outline EU response to hybrid threats by conducting an analysis of the relevant documents and examining the implementations of the policy measures prescribed in those documents.

The crisis in Ukraine and the civil wars in Syria and Libya have turned the Eastern and Southern Neighbourhoods of the EU into an ideal background for the deployment of the wide range of destabilisation tools often referred to as hybrid threats. The possibility that such destabilisation instruments could successfully target EU and NATO members like the Baltic states—or even EU member states that do not belong to the Atlantic Alliance such as Finland and Sweden—has made the formulation of a EU policy against hybrid threats imperative. The 2007 Lisbon Treaty introduced into EU law a collective defence and a mutual solidarity clause which hybrid threats could activate. Specifically, Article 42.7 of the Treaty of the European Union (TEU) states that

If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power.

Article 222 of the Treaty on the Functioning of the European Union (TFEU) contains additional mutual solidarity provisions covering broader range of threats by stating that

The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States.

While—as it is the case for NATO Article 5—the threshold for activating Articles 42.7 and 222 remains open to debate, such unambiguous provisions clearly compel the EU to adopt a unified, proactive approach against hybrid threats.

The Joint Framework on Countering Hybrid Threats

The April 2016 Joint Framework) seeks to bring together existing EU policies into a comprehensive approach aimed at fostering the resilience of the EU, its member states and partner countries while increasing cooperation with NATO on countering these threats.

The document refers to hybrid threats as a ‘mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of

formally declared warfare'. As further stressed in the Joint Framework, hybrid threats 'target critical vulnerabilities and seek to create ambiguity in order to hinder swift and effective decision-making' and embrace a wide array of measures ranging from 'cyberattacks on critical information systems, through the disruption of critical services, such as energy supplies or financial services, to undermining public trust in government institutions or exploiting social vulnerabilities'.¹

As any national security matter, combatting hybrid threats remains primarily member states' responsibility. The Joint Framework, however, forcefully makes the case for a coordinated approach at EU level by using EU policies and instruments. To this end, it identifies 22 operational actions aimed at raising awareness, building resilience, responding to crises and stepping up cooperation with NATO (Table 8.1).

While EU official documents now dedicate extensive attention to the subject, some ambiguity still exists in EU conceptualisation of hybrid threats. For instance, while the Global Strategy maintains a distinction between terrorism and hybrid threats, the Joint Framework suggests that restrictive measures should be used to fight money laundering and the financing of terrorism, thereby subsuming counterterrorism and the fight against hybrid threats. For the purpose of this chapter, the qualifying character of hybrid threats lies in their 'coercive and subversive' nature which remains 'below the threshold of formally declared warfare'.² This conceptualisation effectively captures both disinformation strategies and several of the situations wherein the EU has been using sanctions).

Implementing the Joint Framework

The Actions described in the Joint Framework outline a wide-ranging response to hybrid threats involving a range of different institutions in Brussels and within the member states as well as other international organisations and private sector stakeholders, thereby seeking to formulate a truly comprehensive attempt to enhance the resilience of the EU against hybrid threats. But have EU actions followed suit to those commitments?

In July 2016, the HR released a Joint Staff Document providing the operational protocol against hybrid threats called for by Action 19 of the Joint Framework. The Joint Staff Document fleshes out the decision-making procedures to be adopted to respond to hybrid threats, carving out an important role for the EU Hybrid Fusion Cell as the key source of situational awareness and further explaining the importance

Table 8.1 EU actions against hybrid threats

<i>Action</i>	<i>Actors involved</i>
1. Launch hybrid risk survey to identify key vulnerabilities	MSs, supported by HR and Commission
2. Create EU Hybrid Fusion Cell	EU Intelligence and Situation Centre (EU INTCEN). National contact points to be established by MSs
3. Deliver proactive strategic communications and optimise use of media monitoring	HR, in partnership with MSs
4. Establish Centre of Excellence for 'countering hybrid threats'	MSs
5. Identify common tools to improve critical infrastructure resilience	EU Commission, in cooperation with MSs and private sector stakeholders
6. Diversify energy sources and increase nuclear infrastructure resilience	EU Commission in cooperation with MSs
7. Monitor threats to transport sector	EU Commission
8. Increase resilience of space infrastructure	EU Commission
9. Develop projects to adapt defence capabilities to counter hybrid threats	EU HR, supported by MSs and Commission
10. Improve risk awareness of food and water manipulation and spread of infective diseases	Health Security Committee, Commission and MSs
11. Strengthen national computer security incidents response teams	Commission and MSs
12. Draft public-private partnership for cybersecurity	Commission and private sector stakeholders
13. Improve the cybersecurity of electric networks	Commission
14. Address cyberthreats to networks protecting financial systems	EU Network and Information Security Agency, Commission, and relevant national and international bodies
15. Examine how to respond to cyberattacks across the transport sector	Commission and HR
16. Use action plan on terrorist financing to counter hybrid threats	Commission
17. Reinforce procedures for removing online contents conducive to radicalisation	Commission
18. Launch a hybrid risk survey in Neighbourhood regions	HR, in coordination with Commission
19. Establish a common operational protocol and conduct regular exercises to improve strategic decision-making in response to hybrid threats	HR and Commission

(continued)

Table 8.1 (continued)

<i>Action</i>	<i>Actors involved</i>
20. Examine applicability of Articles 222 TFEU and 42(7) TEU in case serious hybrid attacks occur)	Commission and HR
21. Integrate, exploit and coordinate Common Security and Defence Policy capabilities for military action in countering hybrid threats	HR and MSs
22. Enhance cooperation and coordination with NATO	HR, Commission, NATO

of synchronising EU and NATO parallel activities. The commitment to reinforce NATO-EU partnership was forcefully reinstated by a December 2016 Joint Declaration signed by the President of the European Council, the President of the European Commission and NATO Secretary General.

EU efforts to strengthen strategic communication in its Eastern Neighbourhood, already outlined in the 2015 Strategic Communication Action Plan, also gained momentum as Action 3 identifies strategic communication as a key element for countering hybrid threats. The October 2016 EU Parliament Report on strategic communication, for instance, draws on the Joint Communication and repeatedly mentions disinformation as a key component of Russian hybrid warfare. The second cornerstone of EU response—the Centre of Excellence on Countering Hybrid Threats—has not yet been established at the moment of writing. As a EU member that is heavily exposed to hybrid threats but not included in the North Atlantic Alliance, Finland has expressed interest in hosting the Centre, which may be established by late 2017.

2 EU RESPONSE TO DISINFORMATION OPERATIONS

Information operations have been identified as an especially important destabilisation tool that can serve wider hostile strategic objectives. Disinformation, often popularised as fake news, has become widely discussed in foreign policy circles. US Media and think tanks alike have conducted extensive analysis on misinformation campaigns and their alleged influence on 2016 US elections. EU decision-makers have also grown increasingly aware that disinformation campaigns may pose a threat to EU decision-making processes. The 2017 Dutch,³ French⁴ and

German⁵ elections have made the imperative to act against hostile information campaigns all the more urgent. This section looks at European efforts to counter misinformation targeting EU member states and partners spread by Russian-linked media outlets or online users sympathetic with this narrative. It also briefly examines private-public initiatives that have been created in some European countries to counter these false narratives.

Misinforming the Electorate?

As explained elsewhere in the volume (see Chaps. 11 and 12, by Rogers and Roigas), Russia's misinformation campaign is often seen as part of a broader strategic campaign aimed at weakening EU and NATO unity, which has gained momentum following the EU sanctions imposed on Russia in the wake of the Russo-Ukrainian crisis. The so-called Colour Revolutions in Georgia and Ukraine prompted Moscow to enhance its propaganda machinery to counter the allure of the European project. This effort is epitomised by the opening of new stations of the *Russia Today* TV channel (rebranded RT) and the use of proxy groups in spreading and reproducing its core narrative. The imposition of sanctions following the Russo-Ukrainian crisis has translated into the adoption of more aggressive anti-EU narratives, strengthened by the severe blows suffered by the European project in the last few years. The financial crisis in the Eurozone, the migration crisis and the British decision to leave the Union have all dented the EU's reputation and called into question the viability of the EU, emboldening critics of EU integration. In this context, Russia's messaging 'has proved quite effective, if not necessarily consistent: while often crude and deceitful in terms of content, its delivery is sophisticated, targeted and tailored to different audiences, and capable of exploiting the EU's weaknesses'.⁶

Part of this Russian information offensive is the production and dissemination of content which is sympathetic to Russia's strategic objectives and yet does not seem to be directly spread by the Kremlin, which both increases the credibility of certain narratives and provides Russia with a shield of plausible deniability. As several national elections are to be held in 2017 and 2018, there are concrete risks for democratic processes across the EU. Information operations could influence the elections by manipulating public opinion prior to the vote and undermining trust in the electoral results.⁷ With a view to undermine EU cohesion, Russian operatives are purportedly allying or building bridges with Eurosceptic political

movements. These efforts have been indirectly supported by different European political parties, such as the Front National (FN) in France⁸ and the Northern League and Five Stars Movement in Italy,⁹ all promoting populism and identity politics as ‘a reaction against a wide range of rapid cultural changes that seem to be eroding the basic values of Western societies’.¹⁰

EU Strategic Communication: The Wake-up Call

As ‘strategic communication’ has been used in a variety of sectors ranging from military planning to public relations, it is necessary to briefly define what the term means. Strategic communication is

A systematic series of sustained and coherent activities, conducted across strategic, operational and tactical levels, that enables understanding of target audiences and, identifies effective conduits to promote and sustain particular types of behaviour.¹¹

Based on this definition, it is clear that strategic communication is a bi-directional activity aimed at understanding what the ‘core’ messages of an organisation should be, identifying who the target audiences are and assessing how this message should be tailored. Strategic communication could be categorised under the broad label of ‘soft power’, encompassing all those foreign policy activities aimed at enhancing an organisation’s ability to persuade rather than coerce.

Beginning in 2014, Russia’s ongoing disinformation campaign was a wake-up call for European policymakers, who realised that a prolonged disinformation campaign can poison the political and public arenas, as reiterated by a European Parliament Foreign Affairs Committee’s Resolution in October 2016.¹² This awareness prompted the EU Council to stress ‘the need to challenge Russia’s ongoing disinformation campaigns’ and invite the HR to prepare an action plan on strategic communication.¹³ For the EU, strategic communication is now an ‘important tool in furthering the EU’s overall policy objectives’.¹⁴ Consequently, the European External Action Service (EEAS) has established a dedicated ‘Strategic Communications Division’ leading the EU’s efforts on ‘...the public dimension of European diplomacy and its communication on Foreign Affairs and Security Policy, as well as its external action more broadly’.¹⁵

The 'Action Plan on Strategic Communication' announced by the HR in June 2015 has the overarching aim of improving the public image of the EU while at the same time refuting false stories about the Union. To achieve this aim, the Action Plan is based on three pillars: the effective communication and promotion of EU values towards its Eastern Neighbourhood; the strengthening of the media sector through media capacity building; and the increasing of public's awareness of disinformation and EU's ability to tackle it.¹⁶ From the language of the plan, the EU seems to aim at spreading positive narratives of itself rather than at portraying Russia or other entities in negative terms, thereby engaging in a defensive effort to discredit false stories rather than engaging in counter-propaganda.¹⁷ This strategy differs from the US approach¹⁸ which, since the rise of the so-called Islamic State, is extensively based on counter-propaganda, an approach that had mixed results in gaining the 'heart and minds' of online users.¹⁹

The first tangible result of the Action Plan on Strategic Communication has been the establishment of the EU East StratCom Centre in the summer of 2015.²⁰ The Centre, part of the EEAS' strategic communication department,²¹ has the task of 'developing communication products and campaigns focused on explaining EU policies in the Eastern Partnership region'.²² This task is carried out by ten full-time communication experts speaking several languages including Russian.²³ In January 2017,²⁴ the Centre received an extra 800,000 EUR, reallocated from the existing EEAS' budget, to expand its activity in discrediting false stories not only on Eastern Europe but also on other EU countries which will hold general elections in 2017, such as Germany.²⁵ The Centre has the objective of 'creating synergies between all relevant instruments and fostering close cooperation between all relevant actors'.²⁶ The effort to bring about greater synergy across relevant actors is the 'disinformation/myth busting network', comprising more than 400 experts from over 30 countries who report disinformation articles to the task force (Fig. 8.1).²⁷

As the graphic from the EEAS illustrates, the Centre is built on four pillars: tactical communication, strategic campaigns, project support and myth busting. These objectives resonate with the intentions expressed in the Action Plan, namely to improve the EU's public relations efforts and disclaim false stories. As part of the latter task, the Centre publishes two products aimed at countering Russian disinformation. The first is the Disinformation Review,²⁸ a weekly mailing list aimed at countering false information compiled by the above-cited 'disinformation/myth busting

Fig. 8.1 The East-West StratCom Centre

network' together with the Centre's staff. The second tool to counter Russian misinformation is the Disinformation Digest, which illustrates the differences between the Kremlin's worldviews and Russian independent voices' view by showing 'key trends on Russian social media'.²⁹ A commitment to inform Russian speakers of EU activities is also highlighted by the 2016 launch of the Russian version of the EEAS's website.³⁰ While not representing the official view of the EEAS,³¹ the Disinformation Review and the Disinformation Digest are nonetheless proactive exercises aiming to disprove false narratives.

The Action Plan repeatedly stresses the importance of developing 'effective networks of communicators [as] key to maximising and amplifying the impact and effectiveness of the communication activities undertaken by the East Stratcom Team'.³² To this end, the EU has established and developed contacts with a wide variety of stakeholders, including the NATO Strategic Communications team and the Strategic Communication Centre of Excellence established in Riga in 2013.³³ Both the Strategic Communications Centre of Excellence and the East StratCom Centre are vehicles to developing 'coherent, complementary and interoperable defence capabilities of EU Member States and NATO Allies'.³⁴

Countering Misinformation: The Way Forward

Social media, in combination with widespread diffidence against traditional news sources, have served as a force multiplier for the spreading of fake news. A study of the pro-Trump media sphere during the 2016 US elections argues that these non-traditional media outlets convey a ‘hyper-partisan perspective to the world’. The same conclusions may apply to EU populist movements, also promoting hyper-partisan worldviews that directly or indirectly support Russia’s narratives. Neither the EU nor its member states alone would be capable of countering the hydra-like dangers posed to the EU democratic processes by the spread of false news. It is therefore crucial to build public-private and private-private partnerships which can help counter misinformation while at the same time safeguarding freedom of information. This section briefly outlines three models which have been either adopted recently or could be adapted from law enforcement and counterterrorism operations and could serve as a blueprint to be replicated in countering misinformation.

Firstly, newspapers and media conglomerates should be encouraged in the adoption of a proactive stance against false stories spread online. For instance, in France, ahead of the general election, local and national newsroom have established ‘Cross Check’, a collaborative project conducted together with Google News Lab, ‘to help the public make sense of what and who to trust in their social media feeds, web searches and general online news consumption in the coming months’.³⁵ This model was also followed by the Spanish newspaper *El País*, through its blog ‘Hechos’³⁶ (Facts), created to expose false stories that have gone viral on the web. EU military and civilian authorities can support traditional European media initiatives to counter the spread of fake news through proactive information sharing of all the military and foreign policies that are portrayed in a distorted fashion. The media sector of EU Neighbourhood countries should also be supported in order to create or strengthen credible alternatives to existing Russian and Russia-sponsored media, thereby providing the Russophone population with alternative sources of information in Russian language. Following the Action Plan auspice of improving the capacity of civil society to exercise its role as ‘media watchdog’ and hold ‘Governments to account’, the EU and its member states should also encourage the involvement of civil society in the fight against false narratives. In Lithuania and Finland, for instance, networks of private citizens are serving as an internet army of ‘elves’ countering online trolls’ ‘hate speech and pro-

Russia propaganda' on social media and newspapers' comments sections.³⁷ Finally, following the example of EU policies against terrorist organisations, the EU could adopt a 'follow the money' approach, whereby organisations creating false stories could be hit by sanctions when abroad or simply revoke their license if based in EU member states' territory. Due to its effects on freedom of information, however, coercive action against specific media outlets should only be considered as a last resort.

Such approaches are being either experimented at the time of writing or used effectively in other policy areas and could therefore be adopted to more effectively counter disinformation as well. Effective strategic communication in the age of social networks inevitably requires novel approaches bringing together a wide range of public and private actors.

3 SANCTIONS AS A RESPONSE TO HYBRID THREATS

While the Joint Communication outlines the establishment of novel agencies such as the Hybrid Fusion Cell and Centre of Excellence, EU response to both old and new security challenges inevitably hinges on the existing policy instruments falling under the rubric of the Common Foreign and Security Policy (CFSP) and CSDP. Due to the large size of the EU internal market and the limited military capabilities of the EU, sanctions and restrictive measures have played a prominent role in EU external action and are likely to remain crucial in EU response to hybrid threats and efforts to increase state resilience within its borders, in its Neighbourhood and beyond.

EU Sanctions in a Nutshell

In the past, sanctions were a synonym of general embargoes that did not discriminate among targets within a society. The oil embargo that the UN imposed on Iraq in the early 1990s after the invasion of Kuwait and the last phase of the UN response to the military coup in Haiti are a case in point.³⁸ Comprehensive sanctions, however, were criticised because of their counterproductive effect of harming innocent populations and consolidating the power of ruling elites.³⁹ Consequently, sanctions have changed. Thanks to the evolution of international norms—now allowing for individuals to be accountable before the international community—the Security Council of the UN began to impose sanctions on individuals

and non-state entities.⁴⁰ The practice of ‘targeted sanctions’ has also been widely adopted by the EU.⁴¹

The EU imposes sanctions under three different legal regimes. First, the EU transposes decisions of the Security Council of the United Nations (UNSC), thereby executing sanction regimes adopted by the UN. Second, the Cotonou agreement outlines the possibility for the EU to suspend aid and other forms of cooperation with signatory states when there are human rights concerns in the partner country as outlined by Article 96 of the Agreement. Finally, the EU imposes sanctions as one of its foreign policy instruments under its CFSP.⁴² This chapter focuses on this last set of measures.

The Treaty of Rome established the European Economic Community (EEC) and created the conditions for strong coordination of foreign trade policy by EEC members, but it was only after the Treaty of Maastricht that the EU acquired the possibility to resort to sanctions as a foreign policy instrument. Sanctions are adopted on the basis of Article 29 of the Treaty of the European Union, which allows the Council of Ministers to adopt foreign policy decisions by consensus. Initially, the Council would adopt ‘Common Positions’, later referred to as ‘Decisions’ in the Lisbon Treaty. However, the complex, multi-level structure of the EU has developed into a complex governance system requiring further steps in order to launch and implement sanctions.⁴³

Restrictive measures mainly consist of economic boycotts, financial restrictions, travel bans and arms embargoes. The Council is responsible for measures that alter the functioning of the common market. Economic boycotts entail the prohibition to sell specific products or services to a targeted country, region, company and/or individual. Financial sanctions include the freezing of assets and the prohibition of providing loans and making payments. Article 215 of the TFEU disciplines the matter, giving the power to the Council of Ministers to impose restrictive measures. Member states are responsible for the implementation of arms embargoes and travel bans. Arms embargoes prohibit the sale of weapons and dual-use technologies to specific political actors. Although the EU has produced a list of dual-use goods in 2009 to facilitate the coordination among EU members, it is still up to the latter to monitor and enforce such trade restrictions. Travel bans, which restrict access to the territories of the member states for security reasons, are also implemented by member states.

There are three main documents that discipline EU utilisation of sanctions. First, sanctions are imposed according to tenets illustrated in the ‘Basic Principles’ adopted in 2004.⁴⁴ Second, sanctions are designed and imposed according to ideas that are listed in the ‘Guidelines’, the latest version of which was adopted in 2013.⁴⁵ This document states that the EU has adopted a ‘targeted’ approach, meaning that sanctions were designed to minimise the impact on civilians while increasing the burden on certain actors, namely, targeted individuals, political parties and governmental leaders. Finally, given that imposing sanctions on individuals is extremely detailed, the third document indicates ‘Best Practices’ on the homogeneous implementation of EU decisions across member states.⁴⁶ None of these documents links the utilisation of restrictive measures and sanctions to the countering of hybrid threats explicitly.

The EU Sanctioning Record

The EU’s activity in the field of sanctions has contributed to an enhancement of its visibility on the international stage since the entry into force of the Maastricht Treaty in 1993. Ever since, the EU has increasingly resorted to restrictive measures. In July 2016, for instance, the EU administered 23 autonomous sanction regimes at the same time. Restrictive measures have been imposed to deal with very diverse foreign policy challenges ranging from conflict management and counterterrorism to the promotion of human rights and democracy, as summarised in Table 8.2.⁴⁷

Targeted sanctions in general and EU restrictive measures specifically face both legal and practical challenges. First, as epitomised by the 2008 Kadi case,⁴⁸ the imposition of targeted sanctions on individuals and entities infringes upon rights to property, movement and trade that can be questioned in European and national courts.⁴⁹ In order to combine the protection of individual rights with an effective utilisation of sanctions against both hybrid threats and other challenges, the legal guarantees that are in place at domestic levels need to be extended to the international level as well.

Second, sanctions are challenging to design and implement at the micro-level. Targeted sanctions are extremely difficult to design, tailor, monitor and enforce.⁵⁰ A first prerequisite for effective sanctions design is a perfect knowledge of the society where targets are located. EU sanctions architects, however, have limited intelligence, and the grey area of sanctions busting is difficult to uncover.⁵¹ Moreover, while threats are evolving

Table 8.2 EU restrictive measures divided per type of crisis since 1993

<i>Conflict management</i>	<i>Democracy promotion</i>	<i>Non-proliferation</i>	<i>Post-conflict</i>	<i>Terrorism</i>
Afghanistan	Belarus	DPRK	Bosnia and Herzegovina	Libya
Comoros	Burundi	Iran	Côte d'Ivoire	Terrorist list
DRC	CAR	Libya	Egypt	
Indonesia	China ^a		FRY	
Libya	Guinea		FYROM	
Sudan	Guinea-Bissau		Guinea	
South Sudan	Iran		ICTY indictees	
Transnistria	Myanmar		Libya	
US	Nigeria		Tunisia	
	Sudan		Zimbabwe	
	Syria			
	Uzbekistan			
	Zimbabwe			

^aRestrictive measures on China are only politically binding

and sanction targets are constantly moving, the designing and adaptation of sanctions takes place at a much slower pace.⁵² Third, monitoring capabilities are weak when targets are transnational. This is an inherent weakness of sanctions implementation in the international system, since national authorities do not exercise sovereignty beyond their national borders. The US and the UK are the states that are mostly active in monitoring the implementation of sanctions. Other actors, including the EU, have been less active on that front.⁵³

To date, EU sanctions have been deployed primarily against traditional threats. However, certain mechanisms, practices and experiences can be applied to non-traditional, hybrid challenges such as organised crime, drug trafficking, money laundering and cyberattacks. The next section elaborates on how the use of sanctions can contribute to the fight against hybrid threats.

EU Sanctions Against Hybrid Threats

As the concept of hybridity has only been introduced in EU foreign policy documents in 2016, no European sanctioning regimes to date have been designed with a specific view to fighting hybrid threats. A number of existing EU restrictive measures, however, de facto provide an important

contribution to EU efforts to tackle such challenges. The counterterrorist financing (CTF) policy is a case in point. Under this policy, sanctions are employed against non-state actors involved in coercive and subversive activities that do not meet the threshold of warfare. The EU policy on CTF has two features. First, the EU transposed the decisions made by the UN Security Council on this matter. This meant adopting the so-called 1267 regime, which has evolved into the regime on the al-Qaeda network, the Taliban and ISIL/Da'esh with resolution 1988 of 2009. Second, the EU adopted its own listing in the aftermath of the 9/11 attacks. In December 2001, transposing Security Council 1373 (2001), the Council of Ministers adopted Common Position 931 and Council Regulation (EC) 2580. Common position 931 indicates both the targets (individuals and entities) and the criteria that led to their listing. In practice, there are two lists. The first one imposes a freeze of funds and a travel ban on non-EU citizens, indicating ten individuals and 22 entities as of July 2016.⁵⁴ The second list indicates EU citizens only, which includes 57 individuals and 47 entities.⁵⁵

Sanctions have also been utilised to prevent the derailment of peace-building and state-building processes. In such cases, sanctions enhance resilience by targeting conflict spoilers, defined as those actors that undermine or intend to undermine the stability of a given country. This has occurred in several instances of conflict management situations. For instance, the post-2011 events in the Middle East and North-African region (MENA) show how targeted sanctions can be used to strengthen the resilience of countries in the European Neighbourhood. In the cases of Egypt, Tunisia, Libya and Syria, the EU initially decided to impose sanctions to weaken the incumbent government. In the Libyan case, sanctions were first motivated by the desire to weaken Muammar Gaddafi and later by the intent to sustain the transition towards a new regime.⁵⁶ As of Syria, the EU resorted to coercive measures to persuade Bashar Al-Assad into negotiating with the rebels and the international community. The EU imposed a travel ban on a number of individuals, but Assad himself was initially not targeted (unlike Gaddafi, Ben Ali and Mubarak).⁵⁷ After the call for cooperation fell on deaf ears, the EU extended the list to include Assad and his family and to favour regime change in Syria.⁵⁸ The escalation of the crisis, which led to the imposition of the US/EU coordinated oil embargo on Syria in the summer of 2011,⁵⁹ took place amidst violent confrontations, such as the battle of Aleppo, which led to the death of 500,000 people and the displacement of several millions.

Non-proliferation sanctions could also qualify as actions targeting hybrid threats. In order to deal with this challenge, the EU has regulated trade via dual-use technology approach. From the website of the Commission:

The trade in dual-use items—goods, software and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD)—is subject to controls to prevent the risks that these items may pose for international security.⁶⁰

This means that dual-use items can enable non-state actors to conduct various types of hostile action. The regime is now disciplined by Council Regulation (EC) 428/2009 of 5 May 2009,⁶¹ and it provides a list of items that cannot be exported unless trade is authorised by the competent authority of the member states. To be sure, the export control regime is a regulation that is always in place, while sanctions are extraordinary decisions made by the Council that go under periodic revision (normally 12 months). However, there are two elements that make this comparison worth exploring. First, the listing can be modified by member states in case of security or human rights concerns. Hence, the list is subject to discretionary changes. Second, targeted sanctions often take the form of sectoral measures against specific goods, items and technologies that can be used for societal destabilisation purposes.

In sum, the majority of EU sanctions are not used to counter hybrid threats specifically, but certain applications can be understood in those terms. For instance, sanctions on spoilers and measures to CTF are surely classifiable as such. The next section deals with the shortcomings of EU sanctions, discussing additional ways in which they can be used to combat hybrid threats and enhance state resilience.

A Comprehensive Approach to Sanctions

Sanctions are considered as an exceptional instrument to be used in exceptional times. Short of military action, they are the most common response to serious violations of human rights, unconstitutional change of governments and conventional military threats, such as the recent events in

Ukraine. Sanctions strengthen the resilience of the EU or the international system at large by curbing arms trade, the proliferation of WMD and the financing of terrorism. In order to better combat hybrid threats along the lines envisaged by the EU Joint Framework, a comprehensive approach to sanctions should be developed.

First, the experience accumulated by the EU in its sanctioning history can be used to identify policy areas where trade and export control would reduce the likelihood of attacks against the EU and its allies. For instance, goods and technologies that could be conducive to hostile cyber activities can be included on a list following the model of dual-use technologies as done by the EU in its recent revision rounds in 2009. The 'list-model' could then be extended to other areas where further regulation and more clarity is needed both for private companies to comply and for public regulators to monitor and enforce compliance. Second, since an effective designing and implementation of sanctions requires more information from and concerted action with the private sector, a standing partnership with business is necessary. Banks, industries and trading firms are crucial to implement sanctions. Stronger coordination, or simply information-sharing mechanisms, would facilitate sanction decision-making process and implementation. Better coordination is also needed within the public sector, where a whole-of-government approach is needed to bring together all the actors playing a role in the implementation of sanctions, such as the military, the intelligence community, police, custom agencies, banks and the judiciary. Insufficient communication among these actors may have serious implications on the effectiveness of sanction regimes.

Finally, a comprehensive approach to sanctions must consider the monitoring and enforcement capabilities of public institutions. What happens if sanction-busting activities are discovered? How would state authorities know that sanction-busting schemes are put in place? The answer today is that very little happens outside of the investigations carried out by the Office for Foreign Asset Control (OFAC, see above) of the US. The EU should play a more assertive role in this regard. There are several steps to be undertaken. The first, and most obvious, is pooling and sharing capabilities. Currently, the 28 EU member states have 28 different teams responsible for sanctions implementation, amounting to hundreds of people in total, while only a handful active at the EEAS and the Commission. If states were to second personnel tasked

with implementing sanctions and monitoring compliance to Brussels, both greater efficiency and better coordination would be achieved. A more integrated approach would reduce the amount of time and resources spent in dealing with uneven implementation across the EU. Second, synergies should be built between EU and national institutions with the inclusion of the military and intelligence services (when implementing beyond the borders of the EU) and other enforcing actors (police forces, the judicial system, customs agencies and FRONTEX among others). Lastly, hybrid threats need comprehensive responses. Hence, sanctions need to be integrated within a wider framework that would enable multiple foreign policy instruments to be used coherently with the same objective. At the moment, sanctions are often seen as a stovepiped instrument insulated from CSDP policies such as the launching of crisis management operations. More enforcing power should be delegated to EU institutions in order to address monitoring and enforcement gaps and to fine-tune the interaction between sanctions and other EU policies.

4 CONCLUSIONS

This chapter focused on the EU responses to hybrid threats. While the EU was slow in introducing policy responses to hybrid threats, it eventually envisaged different frameworks aimed at increasing the ability of the EU to cope with destabilisation challenges. EU efforts against misinformation spread from Russia are a case in point. As the Joint Framework introduced only limited novelties in the EU's security architecture, EU external action remains primarily based on the use of pre-existing CFSP and CSDP policy instruments. As a widely used foreign policy instrument, sanctions are especially important in countering hostile strategies aimed at destabilising the EU and the international order at large. To date, however, the potential of sanctions in addressing hybrid threats remains underdeveloped. In order to be effective, both EU strategic communication and sanctions require a tight cooperation between different civilian and military actors. Hence, envisaging effective forms of civil-military interaction is crucial to ensure the effectiveness of the Union's response to destabilisation strategies against EU member states, countries in the European Neighbourhood and the wider international order.

NOTES

1. Joint Framework 2016: 2.
2. Ibid.
3. 'Dutch will count all election ballots by hand to thwart hacking' *The Guardian*, 2 February 2017, Available at <https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking>
4. French election contender Macron is Russian 'fake news' target', *Reuters*, 14 February 2017, Available at <http://www.reuters.com/article/us-france-election-cyber-idUSKBN15S192>
5. 'Hackers lurking, parliamentarians told', *DW News*, 20 September 2016, Available at <http://www.dw.com/en/hackers-lurking-parliamentarians-told/a-19564630>
6. Missiroli, Antonio, Andersson, Jan Joel, Gaub Florence et al. 'Strategic communications – East and South', *European Union Institute for Security Studies* (ISS) p. 30.
7. Bund, Jakob 'Cybersecurity and democracy' *European Union Institute for Security Studies* (ISS).
8. Alina, Polyakova, and Atlantic Council (2016) 'Putinism and the European Far Right'. *Institute of Modern Russia*.
9. See, for instance, Nardelli, Alberto 'Italy's Most Popular Political Party is leading Europe in Fake News and Kremlin Propaganda' *Buzz Feed News*, 29 November 2016, Available at https://www.buzzfeed.com/albertonardelli/italys-most-popular-political-party-is-leading-europe-in-fake?utm_term=.hvM3p8yNJ#.kh7E3ZwKP and Kirchgaessner, Stephanie 'Italy's Five Star Movement part of Growing Club of Putin Sympathisers in West' *The Guardian*, 5 January 2017, Available at <https://www.theguardian.com/world/2017/jan/05/five-star-movement-beppe-grillo-putin-supporters-west>
10. Inglehart, Ronald and Pippa Norris (2016) 'Trump, Brexit, and the rise of Populism: Economic have-nots and cultural backlash' *HKS Faculty Research Working Paper Series* RWP16-026, p. 30.
11. Steve Tatham, Strategic Communications: A Primer, ARAG Special Series 8/28, *Defence Academy of the United Kingdom* (2008), p. 7. Quoted in Paul Cornish, Julian Lindley-French and Claire Yorke, 'Strategic Communications and National Strategy', *Chatham House Report*, September 2011.
12. 'Be aware of Russia and ISIS propaganda, warn foreign affairs MEPs' European Parliament, Foreign Affairs Committee, Press Release, 10 October 2016, Available from <http://www.europarl.europa.eu/sides/>

- [getDoc.do?type=IMPRESS&reference=20161010IPR46530&language=EN&format=XML](#)
13. HR ‘Action Plan on Strategic Communication’.
 14. High Representative of the European Union for Foreign Affairs and Security Policy (HR) ‘Action Plan on Strategic Communication’ 22 June 2015, Available at <http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf>
 15. EEAS Website, available from https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en
 16. Ibid.
 17. see <https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east->
 18. See, for instance, this European Parliament Briefing on US strategic communication to counter foreign propaganda: Naja Bentzen and Lucas Leblanc ‘US strategic communication to counter foreign propaganda’ *European Parliament Research Service*, October 2016, PE 589.812, Available at [http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589812/EPRS_BRI\(2016\)589812_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589812/EPRS_BRI(2016)589812_EN.pdf)
 19. See, for instance, Berger, J.M. ‘Making CVE Work: A Focused Approach Based on Process Disruption’, *The International Centre for Counter-Terrorism – The Hague* 7, no. 5 (2016).
 20. HR ‘Action Plan on Strategic Communication’.
 21. Sabine Lösing, European Parliament written question. Available from <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2016-002156+0+DOC+XML+V0//EN&language=ga>
 22. Ibid.
 23. Ibid.
 24. Ben Knight, ‘EU expands anti-fake-news task force’ DW News, 25 January 2017, Available from <http://www.dw.com/en/eu-expands-anti-fake-news-task-force/a-37265159>
 25. Ibid.
 26. Joint Framework, p. 3.
 27. Ibid.
 28. See an example of the Disinformation Review, available at <http://us11.campaign-archive1.com/?u=cd23226adal699a77000eb60b&cid=9393398338&c=04c6d2a65d>
 29. Available from https://eeas.europa.eu/headquarters/headquarters-homepage_en/9506/Disinformation%20Digest
 30. https://eeas.europa.eu/topics/eu-information-russian_ru
 31. Something demonstrated also by the language and style of the weekly email.
 32. HR ‘Action Plan on Strategic Communication’.

33. European Parliament, Written Answers by the High Representative on behalf of the Commission. Available at <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-002156&language=EN>
34. 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. Available from http://www.nato.int/cps/en/natohq/official_texts_133163.htm
35. <https://firstdraftnews.com/crosscheck-launches/>
36. Available from http://elpais.com/elpais/2017/03/01/hechos/1488366687_423518.html
37. <http://bigstory.ap.org/article/27ce7f001bde4ccb9415ce4a0de74af1/lithuanian-elves-combat-russian-influence-online>
38. David Cortright and George A. Lopez, *The Sanctions Decade: Assessing UN Strategies in the 1990s*. Boulder, Co: Lynne Rienner Publishers, 2000.
39. David Cortright and George A. Lopez, *Smart Sanctions Targeting Economic Statecraft*.
40. Francesco Giumelli, 'Understanding United Nations targeted sanctions: an empirical analysis', *International Affairs*, Vol. 91, No. 6, 2015, pp. 1351–1368.
41. European Union, Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, *The Council of the European Union*, 20 June 2012.
42. Clara Portela, *European Union Sanctions and Foreign Policy. When and Why do they Work?* Routledge, 2010.
43. Francesco Giumelli, 'When private actors comply with public regulations in international security? The case of the targeted sanctions of the European Union', Paper presented at Annual Conference of International Studies Association, Baltimore, 2017.
44. European Union (2004) 'Basic Principles on the Use of Restrictive Measures (Sanctions)', The Council of the European Union, 7 June, available at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010198%202004%20REV%201>
45. European Union, Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, *The Council of the European Union*, 20 June 2012.
46. European Union (2015) Restrictive measures (Sanctions) Update of the EU Best Practices for the effective implementation of restrictive measures, *The Council of the European Union*, 24 March, available at <http://data.consilium.europa.eu/doc/document/ST-7383-2015-REV-1/en/pdf>
47. See also Francesco Giumelli (2013), How EU Sanctions work. A new narrative, Chaillot Paper No. 129, Paris: EU Institute for Security Studies, May.

48. Juliane Kokott and Christoph Sobotta (2012), 'The Kadi Case – Constitutional Core Values and International Law: Finding the Balance?', *The European Journal of International Law* Vol. 23 no. 4, 1015–1024.
49. Paul Eden, 'United Nations Targeted Sanctions, Human Rights and the Office of the Ombudsperson', in Matthew Happold and Paul Eden (eds.), *Economic Sanctions and International Law*, Oxford and Portland, Oregon: Hart Publishing, 2016, pp. 135–170. For implications on commercial contracts, see Mercedes Azeredo da Silveira, *Trade Sanctions and International Sales: An Inquiry into International Arbitration and Commercial Litigation*, Kluivert, 2014.
50. Daniel Drezner, 'Sanctions Sometimes Smart: Targeted Sanctions in Theory and in Practice', *International Studies Review*, Vol. 13, No. 1, 2011, pp. 96–108.
51. Francesco Giumelli and Paul Ivan, 'The effectiveness of EU sanctions – An analysis of Iran, Belarus, Syria and Myanmar (Burma)', *EPC Report*, N. 76, November 2013.
52. Francesco Giumelli, 'Sanctions: moving targets and goalposts', *EUISS Alert*, no. 36, 2015.
53. Francesco Giumelli and Giulia Levi, 'Sanzioni: alle imprese europee la multa arriva dagli Usa', *LaVoce.info* 3 June 2016.
54. Council Decision 2016/1136 of 12 July 2016, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1136&qid=1474969819578&from=EN>
55. Council Common Position 2009/468/CFSP of 15 June 2009, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009E0468&qid=1412596355797&from=EN>
56. [Resolution 1970 of 26 February 2011, S/RES/1970]; [Council Decision 625 of 22 September 2011, 2011/625/CFSP].
57. [Council Decision 273 of 9 May 2011, 2011/273/CFSP].
58. [Council Implementing Decision 302 of 23 May 2011, 2011/302/CFSP].
59. [Council Decision 522 of 2 September 2011, 2011/522/CFSP].
60. <http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/>
61. Replacing Council Regulation (EC) No 1334/2000 of 22 June 2000.