EUISS
EUROPEAN UNION
Institute for Security Studies

PROTECTING EUROPE

The EU's response to hybrid threats

By
Daniel Fiott and Roderick Parkes

CHAILLOT PAPER / 151
April 2019

European Union Institute for Security Studies (EUISS)

100, avenue de Suffren
75015 Paris

http://www.iss.europa.eu
Director: Gustav Lindstrom

© EU Institute for Security Studies, 2019.
Reproduction is authorised, provided the source is acknowledged, save where otherwise stated.

The views expressed in this publication are solely those of the authors and do not necessarily reflect the views of the EUISS or of the European Union.

print

ISBN 978-92-9198-833-4
CATALOGUE NUMBER QN-AA-19-002-EN-C
ISSN 1017-7566
DOI 10.2815/679971

online

ISBN 978-92-9198-832-7
CATALOGUE NUMBER QN-AA-19-002-EN-N
ISSN 1683-4917
DOI 10.2815/712409

Published by the EU Institute for Security Studies and printed in Belgium by Bietlot.
Luxembourg: Publications Office of the European Union, 2019.
Cover image credit: Todd Diemer/unsplash

EUROPEAN UNION
Institute for Security Studies

PROTECTING EUROPE

The EU's response to hybrid threats

By
Daniel Fiott and Roderick Parkes

CHAILLOT PAPER / 151
April 2019

The authors

Daniel Fiott is Security and Defence Editor at the EUISS where he works on European defence, CSDP, the EDTIB, defence industries, defence innovation and hybrid threats. He holds a PhD in Political Science from the Free University of Brussels.

Roderick Parkes is a Senior Analyst at the EUISS where he works on issues relating to international home affairs cooperation – migration, crime and terrorism. He holds a PhD from the University of Bonn.

CONTENTS

EXECUTIVE SUMMARY

The EU takes hybrid threats seriously and has designed an array of policies to counter them. Its main focus is the ongoing crises beyond its borders, throughout its eastern and southern neighbourhoods. In Ukraine and elsewhere, the EU is trying to counter hostile Russian actions. But its countermeasures are focused inwards too as its own member states come under attack. These measures are helping more generally to 'future-proof' the EU itself, to shore up its own internal structures and networks in the face of a rapidly shifting international landscape. They are helping Europe respond to powers such as China and the use of new technologies such as 5G.

These countermeasures now cover everything from the European digital economy to its cyber, maritime, space and energy domains. But they play a particularly important role in three sectors, namely the security of EU borders, its critical infrastructure and the information environment. These three fields constitute quite literally the nuts and bolts of the European Union. Protecting them means defending the very cornerstones of the EU – the three fields are vital to the continued integration of the European economy and to the health of the democratic institutions underpinning it. Predictably, they are the subject of our in-depth case studies.

The case-studies show that the EU must build up its defences, in particular *vis-à-vis* unconventional threats. The response to hybrid threats will never yield to a specific timeframe, meaning that efforts to build resilience will be an ongoing feature of EU external and internal action. The EU has to identify and remedy current vulnerabilities. But it must be constantly on the watch for new vulnerabilities created by actors eyeing a more extensive hybrid campaign. Moreover, apart from the usual slew of policy mechanisms and strategy papers, a truly effective EU response demands nothing short of a new mindset among policymakers and citizens. A solid response is one that can draw on intelligence, financial and human resources but above all good political judgment.

Measured against this yardstick, the EU's response has clearly come some way, not least when it comes to mobilising financial and human resources. However, some familiar sticking points remain. Information-sharing and intelligence exchange between member states and across EU institutions are still a work in progress. Risk assessments are often based on the lowest common denominator (that is, a minimal level of information exchange). Proper response networks are still hampered by a lack of trust. And the EU has yet to properly tap the private sector – let alone to enhance public media literacy. But perhaps the biggest problem is also the oldest: the EU institutions find it difficult to overcome compartmentalised silo mentalities when they devise their strategies and responses to hybrid threats.

This disjointedness is a serious weakness. Adversaries deploy conventional and unconventional tactics as part of an overall strategy to destabilise the EU. No single aspect of the threat facing Europe exists in isolation from others. A disturbance to the EU's critical infrastructure, say, may well appear to be an isolated event. The real challenge for the EU is to join the dots between seemingly staccato events and identify a combined hybrid campaign. And it is here, in this murky field of sleuthing and attribution that the EU will require the key mix - timely and credible intelligence coupled with good political judgment. It goes without saying, therefore, that it would be a mistake to read any of the chapters in this *Chaillot Paper* in isolation from the others - or indeed in isolation from further areas such as cyber defence.

The EU's own sprawling and hybrid nature makes it an indispensable actor for countering

hybrid threats. NATO has grudgingly come to respect the EU as an essential partner in this field and, if the EU can only bring together its capabilities, it could give heft to those current buzz terms – transatlantic security and strategic autonomy. Yet, the Union's hybrid character also leaves it uniquely vulnerable. Hybrid threats demand a cautious balancing act between fundamental rights and security, an open market and a secure economy. And they demand speed and decisiveness. Timing and early response are key, and it is incumbent on the EU institutions and member states to move rapidly. For the EU that means learning to put its money where its mouth is, and calling out a hybrid attack as a hybrid attack.

INTRODUCTION

The notion of unconventional threats that fall under the threshold of military force – a concept which last appeared during the Cold War – has lately made a comeback, albeit under the title 'hybrid threats'. The use of the term 'hybrid threats' has been accompanied by some doubts about whether it actually means anything. There are two main reservations about using the label, and it is worth getting these out of the way quickly.

First, in trying to characterise the non-conventional aspects of modern warfare it is argued that the concept fails to provide a theory that is both comprehensive and operational, and those are precisely the qualities which strategists and policymakers demand from their theories.[1] A whole host of other labels purport to describe hybrid-like challenges more accurately: 'irregular warfare', 'non-linear combat', 'compound warfare', the 'grey zone'. By contrast the concept of hybrid threats is politically subjective, and no single definition can ever be agreed that describes the tactics of such different actors as Russia and Daesh.[2] The proliferation of corrective labels has only added to confusion and contestation over the very idea of hybrid threats. Some argue that organisations like NATO should thus drop the term 'hybrid' altogether and instead focus on how a range of threats connect together to produce a political effect.[3]

It is true that NATO differs from other organisations in its definition of 'hybrid threats'. For example, the European Union understands hybrid campaigns to be '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'.[4] NATO defines hybrid threats as 'those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'.[5] And yet, the different semantic choices of both organisations cannot disguise their basic commonalities. Both speak of state and non-state actors, for instance, even if NATO classifies them robustly as 'adversaries'. These differences of nuance come down to understandable differences of method and mandate.

In fact problems arise only when organisations try to make their definition definitive. Inevitably each differs over issues of attribution, vulnerabilities, capabilities and intentions.[6] One definition may emphasise the combination of conventional and non-conventional means, whereas the other looks at the societal dimension. Thus the Multinational Capability Development Campaign (the 'synchronised use of multiple instruments of power tailored to

1 Élie Tenenbaum, "Hybrid Warfare in the Strategic Spectrum: An Historical Assessment" in *NATO's Response to Hybrid Threats*, ed. Guillaume Lasconjarias and Jeffrey A. Larsen (Rome: NATO Defence College, 2015), pp. 111-12.

2 Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicisation* (London: Hurst Publishers, 2018).

3 Damien Van Puyvelde, "Hybrid War: Does it Even Exist?", *NATO Review*, 2015, https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm.

4 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats", *JOIN(2018) 16 final*, Brussels, June 13, 2018, p. 1.

5 Michael Miklaucic, "NATO Countering the Hybrid Threat", *NATO Allied Command Transformation*, September 23, 2011, https://www.act.nato.int/nato-countering-the-hybrid-threat.

6 Frank G. Hoffman, "Hybrid Threats: Reconceptualising the Evolving Character of Modern Conflict", *Strategic Forum*, no. 240 (April 2009), p. 5.

specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects')[7] rivals the European Centre of Excellence for Countering Hybrid Threats (a 'coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means [...], activities *[that]* exploit the thresholds of detection and attribution as well as the border between war and peace [...] and the aim is to influence different forms of decision making').[8] Despite their best efforts to be rigorous, such definitions are most useful precisely because they allow us to pick and mix.

Second, a fixation on hybrid threats and non-conventional forms of warfare can be an expedient way of ignoring conventional military threats. As one astute analyst observes, while the label 'hybrid' has been useful in stoking policy interest in security issues it only illuminates 'a specific part of what is a much larger evolving puzzle'.[9] The fact that Russia bristles with conventional land and nuclear forces should not be overlooked. Worse: the term 'hybrid 'is considered a conceptual honey trap which attracts attention by dressing up a very old phenomenon as something fresh and new. Commentators are quick to point out that there is nothing new about hybrid threats.[10] Historians have shown that hybrid tactics were used by the likes of Saddam Hussein, Ho Chi Minh, Hizbullah and even the Duke of Wellington.[11] Nevertheless, Russia's hybrid strategy has experienced new life under the 'Gerasimov Doctrine', which has taken on an almost mythological (if overblown)[12] quality in recent years. It has been some time since a military doctrine and tactician have made news in outlets such as the *Financial Times*.[13]

Yet, today's hybrid threats really are different from those of the past, rendered far more deadly not least due to an array of evolving technologies. Whole new vistas have been unleashed by autonomous systems and artificial intelligence. Take unmanned aerial vehicles (UAVs) these are increasingly seen as cheap yet sophisticated systems for reconnaissance, critical infrastructure disruption; and, in the worse cases, they can be weaponised too.[14] Or take the cyber domain.[15] The internet and online networks allow state and non-state actors to unleash their aggression in new ways. They can be used to hack critical infrastructure and democratic processes, launch persuasive disinformation and propaganda campaigns, steal information and unload sensitive data into the public domain. In the worse cases, cyber allows an adversary to take control of assets such as military systems (e.g. unmanned aerial vehicles) and command structures.

In sum, any historically-informed understanding of this particular field of warfare will begin with the observation that a 'hybrid threat' is not just a lumpen mess of non-conventional threats. It is not enough to group together terrorism, civil disobedience, cyberattacks, criminal activities, disinformation campaigns,

7 Patrick J. Cullen and Erik Reichborn-Kjennerud, "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare", *Multinational Capability Development Campaign/NATO Allied Command Transformation*, January 2017, p. 3.

8 "Hybrid Threats", The European Centre of Excellence for Countering Hybrid Threats, January 14, 2018, https://www.hybridcoe.fi/hybrid-threats/.

9 Andrew Monaghan, "The 'War' in Russia's 'Hybrid Warfare'", *Parameters*, vol. 45, no. 4 (Winter 2015-2016), pp. 65-74.

10 Guillaume Lasconjarias and Jeffrey A. Larsen, "Introduction: A New Way of Warfare" in *NATO's Response to Hybrid Threats*, ed. Guillaume Lasconjarias and Jeffrey A. Larsen (Rome: NATO Defence College, 2015), pp. 1-14.

11 Robert Wilkie, "Hybrid Warfare: Something Old, Not Something New", *Air and Space Power Journal*, vol. 23, no. 4 (2009), p. 15.

12 For a corrective of the use of the term 'Gerasimov Doctrine' see Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat", *Critical Studies on Security*, (early view) doi:10.1080/21624887.2018.1441623, https://www.tandfonline.com/doi/abs/10.1080/21624887.2018.1441623?journalCode=rcss20.

13 Henry Foy, "Valery Gerasimov, the General with a Doctrine for Russia", *Financial Times*, September 15, 2017, https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b.

14 "Drones and Countering them in a Hybrid Environment: A Case for EU-wide Regulation on Unmanned Aerial Systems", *Summary Report*, European Centre of Excellence for Countering Hybrid Threats, 2018, https://www.hybridcoe.fi/.

15 Jonathan Zittrain, "'Netwar': The Unwelcome Militarisation of the Internet has Arrived", *Bulletin of the Atomic Scientists*, vol. 73, no. 5 (2017), pp. 300-04.

election meddling, proxy conflicts, fighters without insignia, and call this a hybrid campaign. And yet there is no harm in taking a broad lens to the question of how such challenges converge and whether they are being used to escalate instability. As one expert points out, while there exists a temptation to 'compartmentalise the various modes of war into convenient categories, future adversaries will not gaze through our analytical prism.'[16] The task is to understand what the particular use of hybrid tactics in a given instance reveals about the way an adversary thinks and acts, even if it does not appear to have a clearly defined strategy.[17]

BEYOND SEMANTICS

The reality is that the EU has developed a working definition of hybrid threats and it sees them as a critical issue to be addressed by policymakers working on the Common Foreign and Security Policy (CFSP), the Common Security and Defence Policy (CSDP), the Area of Freedom, Security and Justice (AFSJ) and the Security Union. The EU has been spurred into action by the aggressive behaviour of Russia and its seizure of Crimea, in 2014. This led to fears that Russia may use the same tactics against other former Soviet states and Warsaw Pact members. Additionally, the actions of Daesh in the southern neighbourhood have led the EU to focus on the ways that social media and networks can be used to radicalise Europeans and direct terrorist operations on the European mainland. Finally, cyberattacks emanating from places such as China or Iran and subversive operations by commercial entities have not only disrupted critical infrastructure in Europe (e.g. Wannacry and NotPetya), but have weakened trust in Europe's democratic institutions and processes (e.g. Cambridge Analytica).

The re-emergence of hybrid tactics and the growth of new technologies have at least had the effect of bringing the EU and NATO closer together – surely one of the main benefits. The EU and NATO have signed two Joint Declarations (2016 and 2018) designed to enhance their cooperation on a range of security issues such as maritime security, cyber and hybrid threats. Until even quite recently, a 'grey area' existed between the pair when it came to hybrid threats, and neither organisation could credibly take the lead on the problem. NATO has a mandate for conventional deterrence; the EU deals with crisis management beyond its borders and stewardship of the Single Market. Those Joint Declarations, therefore, are founded on the premise that by combining the efforts and skills of each organisation, that grey area can be rendered a little more black and white – perhaps even closing a gap that might otherwise be exploited by adversaries through the use of hybrid tactics.

More specifically, the EU has developed a range of policy initiatives that are designed to help the Union and its member states respond to hybrid threats and improve its own resilience. In 2013 the EU released a cybersecurity strategy and in 2016 a Directive on the security of network and information systems across the EU was adopted – this Directive (EU 2016/1148 or the 'NIS Directive') was to be fully transposed by all EU member states by 9 May 2018. In addition to the cyber-relevant conclusions of the European Agenda on Security in 2015, the EU presented a Joint Communication entitled 'Resilience, Deterrence and Defence: Building Strong Cyber Security for the EU'[18], which included initiatives such as a strengthening of the EU Agency for Network and Information Security (ENISA)

16 Hoffmann, "Hybrid Threats: Reconceptualising the Evolving Character of Modern Conflict", p. 8.

17 Lawrence Freedman, "Ukraine and the Art of Limited War", *Survival: Global Politics and Strategy*, vol. 56, no. 6 (2014), pp. 7-38.

18 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU", *JOIN(2017) 450 final*, Brussels, September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&rid=3.

and a blueprint for a coordinated response to large-scale cybersecurity incidents and crises in the EU.[19] The EU's efforts are not confined to cybersecurity, however.

In 2015 the EU established an 'East StratCom Task Force' to combat disinformation directed against Europe by the Russian government and media sources.[20] Task forces on strategic communication were later established for the South and the Western Balkans. On 6 April 2016, the EU outlined a joint framework on countering hybrid threats, which, among other things, established the 'Hybrid Fusion Cell' a hub for analysing potential hybrid threats in the EU's intelligence and situation centre (INTCEN).[21] An 'EU Hybrid Playbook' laid the first steps towards a system of coordination at the EU and national levels in case of a hybrid attack.[22] In June 2016, the High Representative of the Union for Foreign and Security Policy and Vice-President of the European Commission (HR/VP) released the EU Global Strategy. Its mantra was the 'protection of Europe' - through crisis management, border protection and efforts to counter extremism, cyberattacks and disinformation along the 'nexus' between internal and external security.

It spurred the EU to take stock of its joint framework for countering hybrid threats[23] and enhancing practical responses to hybrid threats. In 2017 the EU not only published an action plan to tackle chemical, biological, radiological and nuclear risks,[24] but a range of exercises were organised too. On 28 September 2017, the EU launched a parallel and coordinated exercise (PACE17) on a fictitious scenario in order to test the EU's situational awareness, reaction time, communications channels – and to learn some lessons. From 5-23 November 2018, an 'EU Hybrid Exercise 2018' was organised. It should also be noted that in 2016 the European Defence Agency (EDA) had organised a table-top exercise on a fictitious hybrid crisis situation. All of the measures taken by the EU since 2015 were summed up in a joint communication on increasing resilience and countering hybrid threats and further action points were tabled.[25] And, finally, last December the EU published its approach to tackling disinformation.[26]

This is not an unalloyed story of progress. Alongside the proliferation of EU measures (see Figure 1 on page 9) there is a proliferation of national approaches. There is a strong case for greater coherence between national strategies, not least in order to identify best practices – there is much to learn from certain EU member states. Beyond the strategies, how far has the EU come in preventing and responding to hybrid threats, as opposed to just writing about the issue? Given that hybrid threats represent a combination of different threats and tactics, what are the most effective methods and strategies for tackling multiple threats

19 European Commission, "Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises", *C(2017) 6100 final*, Brussels, September 13, 2017, https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF

20 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan on Strategic Communication", *Ares(2015)2608242*, June 22, 2015, http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf.

21 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication establishing a Joint Framework on Countering Hybrid Threats", *JOIN(2017) 18 final*, Brussels, April 6, 2016.

22 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats – 'EU Playbook'", *SWD(2016) 227 final*, Brussels, July 5, 2017.

23 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report on the Implementation of the Joint Framework on Countering Hybrid Threats – A European Union Response", *JOIN(2017) 30 final*, Brussels, July 19, 2017.

24 European Commission, "Action Plan to Enhance Preparedness against Chemical, Biological, Radiological and Nuclear Security Risks", *COM(2017) 610 final*, Brussels, October 18, 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf.

25 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats", *JOIN(2018) 16 final*, Brussels, June 13, 2018.

26 European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on an Action Plan Against Disinformation", *JOIN(2018) 36 final*, Brussels, December 5, 2018, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

simultaneously? How can the EU help improve coordination between member states on hybrid threats, especially in a rapidly changing and deteriorating security landscape? Are the EU and its member states on course to developing a common approach to early warning and risk analysis? What are the EU's institutional and societal strengths in the face of hybrid threats and conventional security challenges? Is the Union linking early warning with early action?

THE PURPOSE OF THIS STUDY

A few notes on what this *Chaillot Paper* is and what it is not. First, it is not interested in debating conceptual issues. It does not engage in any further debate about the merits of the term 'hybrid threats'. Quite simply: the term 'hybrid threats' is already being used and understood by EU officials and government representatives to capture a range of non-conventional security challenges. Whether in healthcare and/or transport, the 'hybrid' label is encouraging staff in various EU bodies to give more consideration to the security aspects of their respective portfolios than has perhaps been the case in the past. An annex containing a glossary provides further background information.[27]

Second, this *Chaillot Paper* will not delve into the vulnerabilities of EU member states. Again, this could be positively unhelpful. In conducting the analysis for this paper, we consulted a range of primary materials. We conducted semi-structured interviews with EU officials and government representatives. And we co-organised a simulation and conference on 28 February – 1 March 2019 in Bucharest. Another workshop and simulation on transboundary crises and hybrid threats was organised in Brussels on 4 April 2019.[28] This is not the place to rehearse vulnerabilities revealed in confidence.

Third, this *Chaillot Paper* does not simply provide a list of EU initiatives that have already been developed. Indeed, the aim of this study is to provoke ideas for further action on hybrid threats and to identify avenues for further coordination between EU bodies and member states. In essence, this study wants to provide the reader with practical and operational insights on how best to counter hybrid threats. It shares best practices and uncovers possible ways of improving coordinated EU approaches to hybrid threats. But, just as this publication is not a vulnerability assessment, nor does it deal with the possible development of aggressive hybrid capabilities by the member states, let alone by the EU.

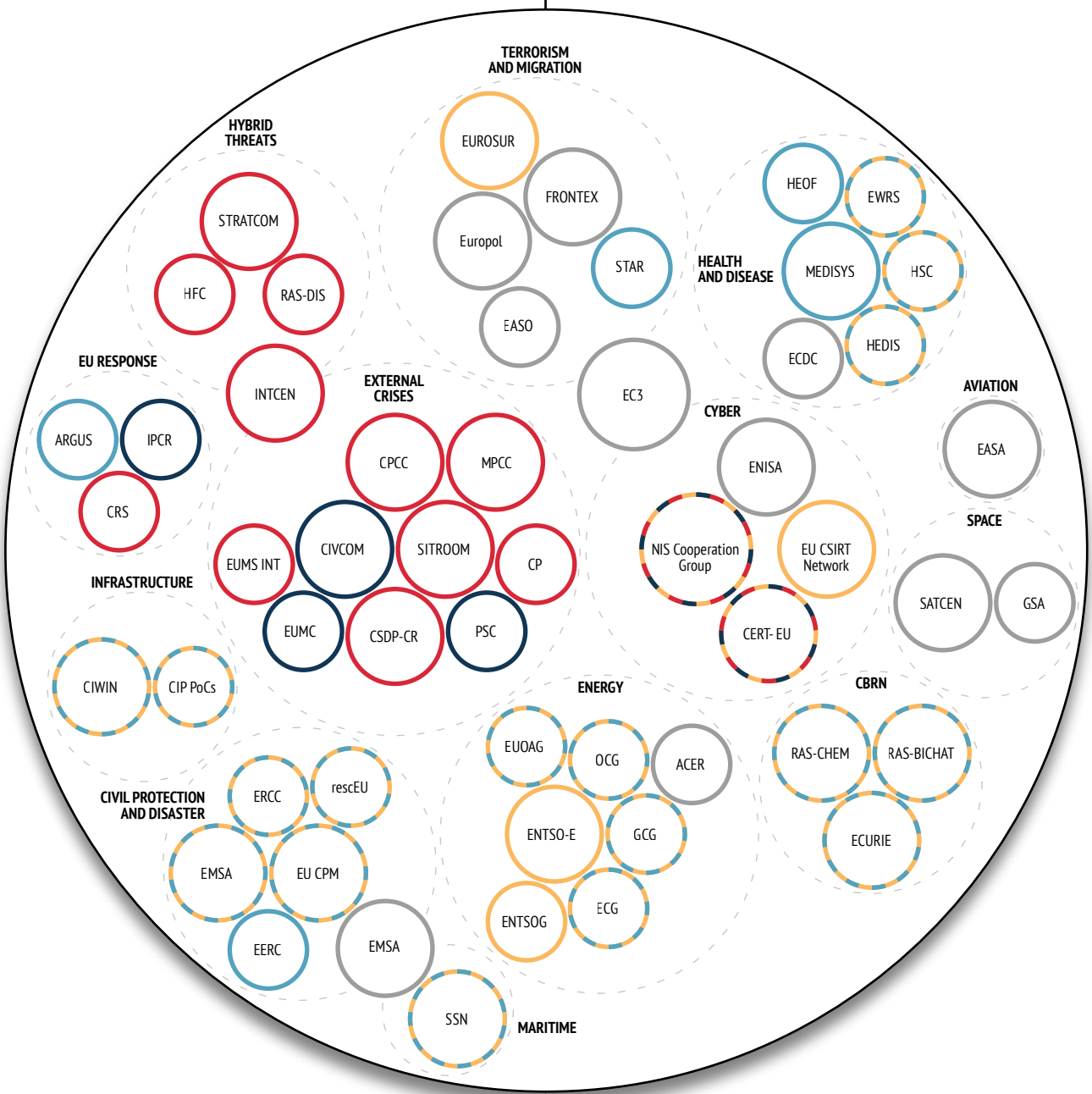
We look at three indicative areas: these deal with the EU's territorial, physical and institutional infrastructure. *Borders* are rendered vulnerable because of increased migration to Europe and by the 'weaponisation' of cross-border flows. *Critical infrastructure* is targeted as a means of upsetting the civilian population with energy shortages, digital and financial disruption, and delays to transport and healthcare. *Disinformation* poisons democratic processes and institutions, as well as trust in the media and government. Each chapter provides an overview of the subject matter and outlines EU policy developments. What this paper does do is try to answer the big question: in what practical ways can the EU prevent and respond to hybrid threats?

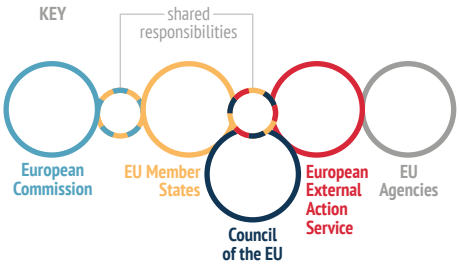
27 The authors would like to thank Federica Fazio for helping compile the glossary and for assistance with data collection in chapter three.

28 The Institute would like to thank the Romanian Presidency of the Council of the EU and the General Secretariat of the Council of the EU for their support in organising high-level conferences on hybrid threats in 2019. See EU Institute for Security Studies (EUISS) , "Facing Hybrid Threats through Consolidated Resilience and Enhanced Strategic Communication", Bucharest, February 28, 2019, https://www.iss.europa.eu/content/facing-hybrid-threats-through-consolidated-resilience-and-enhanced-strategic-communication; and EUISS, "From Sense-making to Decision-making: Sharing Experiences on the Management of Transboundary Crises in the EU", Brussels, April 4, 2019, https://www.iss.europa.eu/content/sense-making-decision-making-sharing-experiences-management-transboundary-crises-eu.

Figure 1 – The EU's crisis response architecture

An overview





abbreviations overleaf

ACER
Agency for Cooperation of Energy Regulators

ARGUS
European Commission Coordination System

CERT- EU
EU Computer Emergency Response Team

CIP PoCs
Critical Infrastructure Protection Points of Contact

CIVCOM
Committee on Civilian Aspects of Crisis Management

CIWIN
Critical Infrastructure Warning Information Network

CP
Crisis Platform

CPCC
Civilian planning and Conduct Capability

CRS
Crisis Response System

CSDP-CR
CSDP and Crisis Response

EASA
European Aviation Safety Agency

EASO
European Asylum Support Agency

EC3
European Cybercrime Centre

ECDC
European Centre for EU Disease Prevention and Control

ECG
Electricity Coordination Group

ECURIE
European Community Urgent Radiological Information Exchange

EERC
European Emergency Response Capacity

EMSA
European Maritime Safety Agency

ENISA
EU Cybersecurity Agency

ENTSO-E
European Network of Transmission System Operators for Electricity

ENTSOG
European Network of Transmission System Operators for Gas

ERCC
Emergency Response Coordination Centre

EU CPM
Civil Protection Mechanism

EU CSIRT Network
EU Computer Security Incident Response Teams

EUMC
European Union Military Committee

EUMS INT
EU Military Staff Intelligence

EUOAG
EU Offshore Oil and Gas Authorities Group

Europol
EU Agency for Law Enforcement Cooperation

EUROSUR
European Border Surveillance System

EWRS
Early Warning Response System for Communicable Diseases and Outbreak of Unknown Aetiology

FRONTEX
European Board and Coast Guard Agency

GCG
Gas Coordination Group

GSA
European GNSS Agency

HEDIS
Health Emergency and Disease Information System

HEOF
Health Emergency Operations Facility

HFC
Hybrid Fusion Cell

HSC
Health Security Committee

INTCEN
EU Intelligence and Situation Centre

IPCR
Integrated Political Crisis Response

MEDISYS
EU Information Scanning Tool

MPCC
Military Planning and Conduct Capability

NIS Cooperation Group
Network and Information Systems

OCG
Oil Coordination Group

PSC
Political and Security Committee

RAS-BICHAT
Rapid Alert System - CBRN Agents

RAS-CHEM
Rapid Alert System - Chemical

RAS-DIS
Rapid Alert System- Disinformation

rescEU
Reserve Operational Capacities at the Union level

SATCEN
EU Satellite Centre

SITROOM
Situation Room

SSN
SafeSeaNet

STAR
Strategic Analysis and Response Centre

STRATCOM
Strategic Communication Taskforces

CHAPTER 1

FLOWS AND BORDERS

Preparing for a hybrid attack at the border

'Little green men'. When people think of hybrid border threats, they likely envisage the Russian soldiers who seeped across the border into Ukraine in unmarked green uniforms in 2014. Border incursions and land grabs by unmarked soldiers have a long history – the method was used first against Colombia in the 1930s (by the Peruvians) and then in Kashmir in 1999 (Pakistanis).[1] But this, the 'classic' hybrid border attack, is not uppermost in the mind of EU officials when they think of hybrid border threats. Russia or Turkey are unlikely to launch such an attack on the territorial integrity of an EU member state. And if they did – around the Suwalki Gap, say, or on one of the Aegean islands – the response lies largely outside EU competencies. Territorial defence for almost all EU member states is a task for NATO.[2]

The EU's competencies lie instead in managing the borders of the Schengen Area, the EU's passport-free travel zone. The Union's powers in this field are laid out in Title V of the Treaty on the Functioning of the EU (TFEU). Article 67(2) TFEU gives the EU the power to frame a common European borders policy, and Article 67(3) charges it with providing security within these borders. This traditionally means preventing cross-border crime and irregular migration. The hybrid threat derives from their potential 'weaponisation' by hostile powers. The response requires the EU to monitor the flows of migrants and criminals, of goods and waste, weapons and information, and it requires border guards and law-enforcement officials to close down the avenues for hostile powers to exploit the vulnerabilities of the EU's globalised economy.

THE THREAT TO THE EU'S BORDERS

The Schengen Area covers 4 million km² of Europe and is fringed by the three usual border types – land, sea and air. Each of the three border types is clustered in a different part of the passport-free travel area. As a result, the EU is facing three relatively distinct clusters of hybrid threats, each associated with one of the three border types, the specific flows encountered at that type of border, and a geographically-proximate sponsor state or terrorist group.

Along the southern flank of the EU, the maritime border stretches from the Aegean to the Western Mediterranean. The most obvious threat here is posed by Daesh and other terrorist groups with roots in the Middle East and North Africa region. These groups have displaced people across the Arab World, and then

1 Dan Altman, "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries", *International Studies Quarterly*, vol. 61, no. 4 (2017), pp. 881-91.

2 And the treatment of regions inside the EU with secessionist ambitions and of ethnic minorities falls to the Council of Europe (COE) and the Organisation for Security and Cooperation in Europe (OSCE).

exploited the migration flows themselves, sometimes taxing migrants for financial gain, sometimes smuggling family members to safety to increase their hold on local territory. They have politicised the flow of people into Europe, hoping to trigger anti-Muslim feeling and to fuel left- and right-wing terrorism. As for transit countries such as Turkey, they have been accused of accommodating terrorist groups. Turkey has also shown an interest in using migration flows not just for political leverage *vis-à-vis* the EU, but to increase its territorial holdings in Kurdish areas. It has seemingly exploited the tensions in the Aegean with Greece, while also pushing Kurdish refugees into the EU and offering to secure 'safe zones' to its south.

The cyberattack which hit Maersk in 2017 cost the Danish shipping giant a little over €250 million.

To the east, the EU shares a long land border with three members of the 'Eastern Partnership' - Ukraine, Belarus and Moldova – as well as with Russia. The vulnerabilities along this border are largely inherited from the Soviet domination of the area. Poland and its neighbours were formerly on the frontline to Western Europe, and their most advanced border infrastructure was to the West. By contrast their eastern borders were built for transit, and communities there still tend to straddle both sides of the border. The EU is committed to ensuring no new iron curtain descends on the East. But this commitment to a light-touch border regime may invite exploitation by Moscow, which has not been shy to use criminal networks for geopolitical purposes. Criminal motorcycle gangs and smugglers are known to be closely linked to the government. The danger is heightened in spots where the EU shares a border with Russia itself and where the demarcation is not always accepted. Member state border disputes are a field where the EU specifically does not have competence (Article 77(4) TFEU).

Lastly, in the EU's north-west lie the heavily globalised border hubs. Western Europe is home to major airports Charles de Gaulle (Paris), Frankfurt and Schiphol (Amsterdam), as well as cargo ports – Rotterdam, Antwerp, Hamburg. A small disruption in any of these has massive repercussions. A drone incident like the one at Gatwick airport in 2018 cost a single airline €17 million in passenger welfare costs and lost revenue. The cyberattack which hit Maersk in 2017 cost the Danish shipping giant a little over €250 million, not including the ramifications for other firms in its global supply chain.[3] Maersk was hit by malware hidden in an electronic tax return in Ukraine, a sign of the vulnerability of networked systems. Threats at these borders come as much from inside the EU as outside, and may be physical or virtual. Air and sea ports house expensive infrastructure such as liquefied natural gas (LNG) refineries, for instance, leaving them vulnerable to so-called insider threats by employees.

The EU's threat assessors: Frontex and co.

Frontex leads on border matters, and in 2016 it gained new powers to carry out assessments of the EU's border vulnerabilities. Each year, it sends out questionnaires to national border authorities helping them work through their shortfalls, before simulating crisis scenarios in a select few member states. The trouble is that national authorities are reluctant to share information about their vulnerabilities with the EU and its agencies. Member states fear both leaks and censure. Governments have therefore insisted that the Frontex vulnerability assessments should remain narrow in scope and that the results should not be shared widely – even with other member states. This makes

3 Richard Milne, "Moller-Maersk Puts Cost of Cyber Attack at up to $300m", *Financial Times*, August 16, 2017, https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff.

it extremely difficult for Frontex to produce a comprehensive picture of Schengen's vulnerabilities. The borders agency has focused its efforts instead on creating a database which allows member states to see whether they meet common norms when it comes to staffing levels and capabilities.

The Commission is now incentivising member states to be more forthcoming about their vulnerabilities. It has announced that it will base future procurement decisions on the results of the Frontex vulnerability assessments.[4] But if member states are indeed slowly opening up, it is probably for a different reason. They hope to influence Frontex and the Commission. The Commission has begun a three-step process to create a European border strategy. In March 2018, it published pointers on 'Integrated Border Management'. Frontex has just drafted a capability-development strategy to match. And each member state is drawing up a relevant national strategy. Governments, particularly in the east and south, see in this a means to bring hybrid vulnerabilities onto the EU agenda. Schengen, it should be remembered, began life as an initiative of five north-western member states, and its strategic outlook is still largely attuned to Luxembourg's priorities circa 1995.

A whole string of EU member states is eager for Frontex to step up its response to hybrid threats. And it just so happens that they have been hosting the EU presidency between them since 2017. Estonia, Bulgaria, Austria, Romania and Finland have all experienced acute border vulnerabilities. Tallinn is currently constructing a fence designed to reinforce its eastern border after an Estonian official was abducted by Russians there in 2014. Bulgaria suspects Russia of supporting anti-migrant vigilantes with equipment and anti-Muslim rhetoric. Sofia also had to watch as Turkey withdrew from a repatriation agreement in 2015 only to push large numbers of Iraqi Kurds across the border into Bulgaria. As for Finland, in 2016 it experienced a sudden influx of Afghan, Bangladeshi and Indian migrants from Russia, who were presumably being helped across the border by Russian security services.

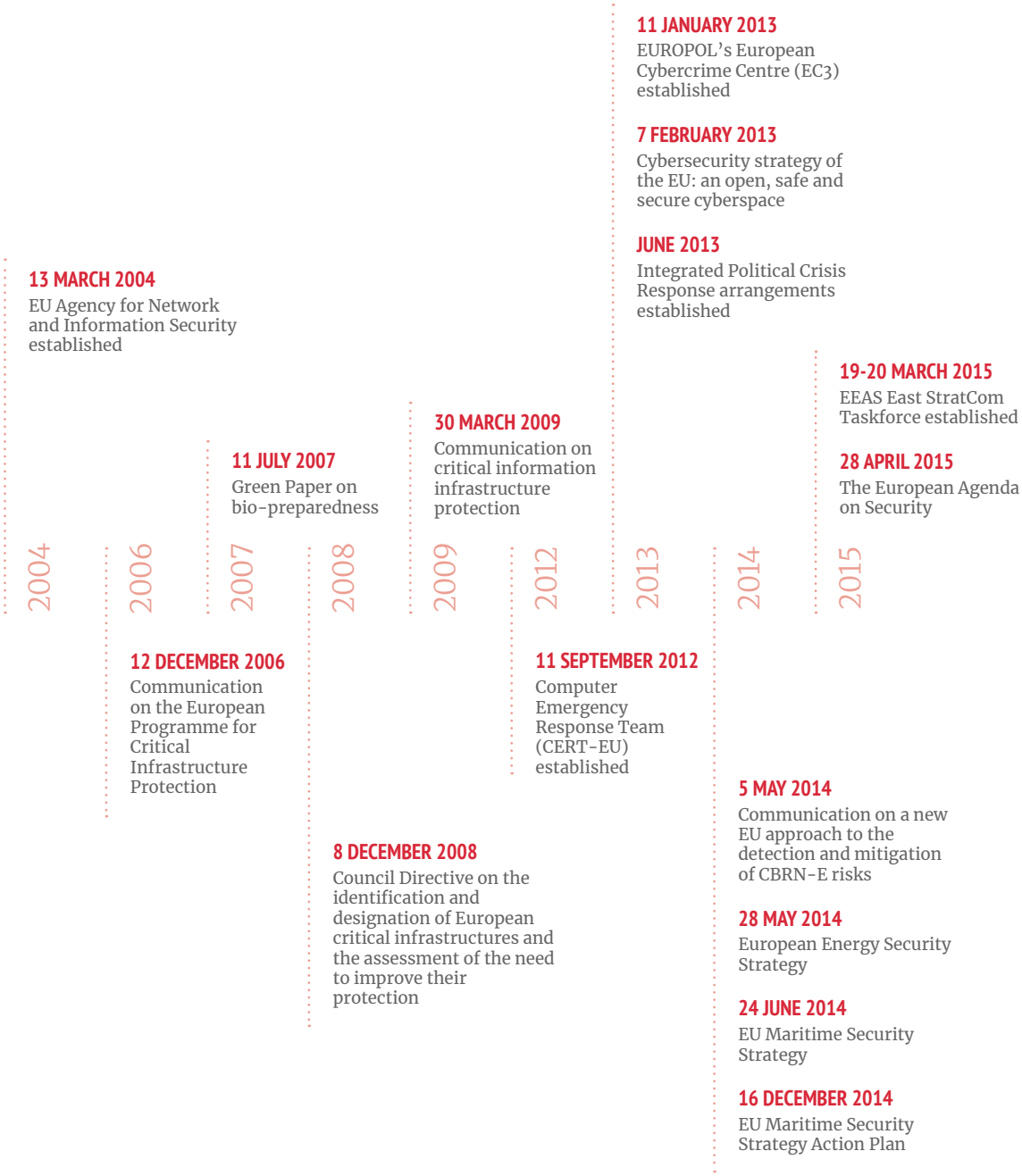
Most of these states have a strong history of border guarding. Their models may be civilian, but they often bear the hallmarks of the heavily-militarised East-West Cold War division. In some cases, the border services would even revert from the ministry of the interior to the defence ministry in the event of an attack. Austria has a history of neutrality of course - but precisely because of this history, it has often deployed its troops in domestic tasks such as border support. Likewise Finland was able to maintain military patrols at its eastern border to the Soviet Union by mirroring them at its Western border to Sweden and Norway. Some of these five states are either newcomers to Schengen or, in the case of Bulgaria and Romania, still waiting to enter. They all feel that they have a new perspective to bring to Schengen's original north-western core.

Why are the EU's borders a target?

In opinion polls, Europeans still rank the Schengen free movement regime as one of their favourite aspects of EU integration. Abroad, too, the EU's most popular policies involve creative approaches to border liberalisation – visa freedom, 'mobility partnerships', enlargement. The fact that the EU's border regime enjoys high international standing makes it a target for attack by rival powers. Liberal border regimes like the EU's can be readily portrayed as a threat to domestic and international security, and Schengen is a particularly experimental version of border liberalisation. This allows revanchist states like Russia or Turkey to play

4 This creates a financial inducement for member states to be properly open about their border shortfalls: if member states show Frontex that they lack a certain border capability, then the EU will finance its purchase. Under the new Multi-annual Financial Framework, the EU would pour considerable new resources into border management. The Commission has proposed to dedicate €21 billion to border management, including a new Integrated Border Management Fund (IBMF) worth more than €9 billion. But there is a risk that these inducements might backfire - that member states exaggerate their shortfalls in order to get access to European funds.

Figure 2 – Hybrid threat-related initiatives



6 APRIL 2016
Communication for a joint framework on countering hybrid threats: an EU response

APRIL 2016
EEAS Hybrid Fusion Cell established

27 APRIL 2016
Regulation on the General Data Protection Regulation

25 JUNE 2016
A Global Strategy for the EU's Foreign and Security Policy

6 JULY 2016
Directive concerning measures for a high common level of security of network and information systems across the Union

2016

7 JULY 2016
EU operational protocol for countering hybrid threats ('EU Playbook')

8 JULY 2016
Joint declaration on EU–NATO cooperation

14 SEPTEMBER 2016
Regulation on the European Border and Coast Guard

26 OCTOBER 2016
Space Strategy for Europe

14 NOVEMBER 2016
Implementation Plan on Security and Defence

6 DECEMBER 2016
42 common proposals for EU–NATO cooperation endorsed by the Council of the EU

11 APRIL 2017
European Centre of Excellence for Countering Hybrid Threats established

7 JUNE 2017
Communication on a strategic approach to resilience in the EU's external action

19 JUNE 2017
Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox')

7 SEPTEMBER 2017
EU CYBRID 2017 cyber defence exercise

13 SEPTEMBER 2017
Proposal for a Regulation to establish a framework for the screening of foreign direct investments into the EU

2017

13 SEPTEMBER 2017
Joint communication on resilience, deterrence and defence: building strong cybersecurity for the EU

28 SEPTEMBER – 4 OCTOBER 2017
Parallel and Coordinated Exercise (PACE17) on cyber and hybrid threats

18 OCTOBER 2017
Action plan to enhance preparedness against CBRN security risks

NOVEMBER 2017
EEAS StratCom South established

NOVEMBER 2017
EEAS StratCom Western Balkans Taskforce established

11 DECEMBER 2017
Council decision establishing Permanent Structured Cooperation

30-31 JANUARY 2018
European Commission (DG SANTE) table top exercise (Exercise Chimera) on hybrid threats

6 FEBRUARY 2018
Cyber platform for education, training, evaluation and exercise in the ESDC established

22 MARCH 2018
European Council conclusions on the Salisbury attack

26 APRIL 2018
Communication on tackling online disinformation: a European approach

13 JUNE 2018
Report on the implementation of the joint framework on countering hybrid threats

2018

26 JUNE 2018
Communication on increasing resilience and bolstering capabilities to address hybrid threats

10 JULY 2018
Joint declaration on EU–NATO cooperation

5-23 NOVEMBER 2018
EU Hybrid Exercise 2018

5 DECEMBER 2018
Action plan against disinformation

10 DECEMBER 2018
EU Agency for Cybersecurity established

19 FEBRUARY 2019
Council conclusions on securing free and fair European elections

MARCH 2019
Rapid Alert System for disinformation established

2019

a double game. They can politicise Schengen's border-bending attributes to portray the EU as a threat to international stability but also as a precedent to challenge their own, post-imperial borders. Likewise Daesh may politicise the EU's experiments with territoriality in a bid to gain legitimacy for its own state-like attributes.[5]

All this makes the EU's border system a target in its own right. Still, the present chapter should not be read in isolation from the other two case-studies in this *Chaillot Paper.* A hybrid attack at the Schengen border would almost certainly link to the other two phenomena dealt with in this paper – to vulnerabilities in the EU's critical infrastructure ('nuts and bolts') and its political infrastructure ('hearts and minds'). Borders are by nature peripheral. But one typical characteristic of hybrid warfare is that its 'centre of gravity' is the enemy's civilian population. And so a hybrid action confined to the border – say an attack on infrastructure there - is unlikely to have the desired impact on the popular imagination. To be effective, a border attack would likely need to link up to a political disinformation campaign or an attack on critical infrastructure. It must play on societies' fears.

This has already come to pass. The terrorist attacks in Paris in November 2015 seemed designed to undermine popular confidence in EU border control. The perpetrators went out of their way to register at refugee centres on their way across Europe: they wanted EU citizens to believe the migration flows had been infiltrated by foreign terrorists. In fact the perpetrators were EU citizens returning from the fighting in Syria. Two months later it was Russia playing the game. Russian television reported that a Russian-German girl, 'Lisa', had been beaten and raped in Berlin by recently-arrived immigrants of Middle-Eastern origin. The story was false, but it did not prevent the Russian foreign minister from accusing German authorities of a cover-up or Russian-Germans from taking to the streets in protest. Frontex faces a constant battle over its image, and the European External Action Service (EEAS) now deals with borders and migration in its strategic communications.

It must be remembered also that Schengen itself is part of a critical infrastructure system which criss-crosses the whole territory of the EU. Schengen operates a 'networked border' system. Schengen members are able to loosen their border controls because someone else – another member state, a third country, an airline, a bank – has carried out a document check in advance of the traveller's arrival. Documents are checked against a whole panoply of identity databases. The EU is currently centralising and interlinking these databases, leaving the system prey to a hack attack or disinformation operation. Physical attack is not inconceivable, either. Very few sites in Europe have the right physical attributes to house large databases – a secluded environment, often near to a lake for cooling purposes. The EU's sites are clustered in Strasbourg, backed up in Austria, and hundreds of miles from the EU agencies which actually manage them.

POLICY RESPONSE: ADDRESSING FOUR BORDER WEAKNESSES

Policymakers have identified four different sets of problems with the EU's border resilience: in the way it manages its borders, the EU has shown itself to be too narrow, too fragmented, too blurred and too top-down. These vulnerabilities are being plugged.

5 Deon Geldenhuys, "The Islamic State (IS): An Exceptional Contested State", *Austral: Brazilian Journal of Strategy and International Relations*, vol. 6, no. 12 (2017), pp. 9-35.

Narrow: expanding oversight of EU borders

The EU's first vulnerability derives from the fact that the Schengen border is extremely long and spans the external sea and land borders of 26 European nations. It winds its way round the Portuguese Azores and Spanish Canaries, taking in the jagged Greek islands and skirting the Russian exclave of Kaliningrad. It inherits many of its member states' territorial anomalies. And, thanks to the way Schengen was initiated by a sub-set of EU member states, it sometimes winds its way through the territory of the EU itself. The logical step for the EU has been to increase surveillance across the entirety of the Schengen border and strengthen common operational procedures for all EU members.

Some years ago, the EU put in place a comprehensive border surveillance system run by Frontex's Situational Awareness and Monitoring Division. The Eurosur Fusion Service (EFS) today uses this surveillance information as the basis for more than a dozen analytical products (including vessel-tracking and maritime simulations). EFS is capable of identifying a suspicious vessel in the Mediterranean by the fact, say, that it has switched off its ship-to-shore communications. To chart the vessel's likely course towards Europe, EFS will use weather simulations and data from previous suspicious crossings. Frontex's European Patrol Network and maritime Joint Operations will supplement this picture by flagging up yachts sitting unusually heavily in the water and other suspicious sightings. EFS also makes use of the EU's military capabilities, including the Madrid-based Satellite Centre to which the borders agency has seconded staff.

The EU complements Frontex's surveillance capabilities with other European agencies and institutions. There is the Migrant Smuggling Centre, an intelligence-led hub housed in Europol. And there is the EEAS's Intelligence and Situation Centre (INTCEN) which analyses threats beyond the EU's border which may impinge on the EU. The Commission's Directorate General for Human Resources and Security (DG HR) is often overlooked in favour of DG HOME, the Directorate General for Home Affairs. But DG HR specifically assesses the risk posed to EU staff and buildings, and this is important because it takes into account the fact that the EU itself can be a target of smugglers and criminals. For crisis situations, there is also the Integrated Political Crisis Response (IPCR) the EU's response coordination mechanism. The member states chose to trigger the IPCR in 2015, and the IPCR began producing weekly situational reports on migration flows jointly with the Strategic Analysis and Response (STAR) capability in DG HOME.

All of these various systems have had teething problems. These reveal some fairly basic deficits in the capacity of EU institutions and member states even to agree on what they are looking at. Take those weekly situational reports. They were plagued by different national interpretations of statistical definitions. There were no clear categories to differentiate between irregular migrants who had been picked up on islands and those on the mainland of a member state – something important in Greece. Nor could authorities agree what day events had occurred. Most national border authorities logically defined a calendar 'day' from 12am, but some started the clock when their first shift began – 5am, say. It also turned out that some small Schengen territories – small islands – had no capacity to input data into Schengen systems or indeed to properly apply its rules. And there was even a certain degree of confusion about which states are even included in the Schengen Area for statistical purposes.[6]

With those problems fixed, the EU is under pressure to expand its borders code so as to ensure that member states not only watch their borders, but also know how to respond to the problems they flag up. The Schengen Borders

6 Romania and Bulgaria are not members of Schengen, but will likely be included in the area for the purposes of the Visa Information System, leading to statistical complications.

Code (SBC) already gives detailed guidance of course, but it applies mainly to official border crossing points (BCPs). 'External borders may be crossed'," says Article 5(1) of the SBC somewhat hopefully, 'only at border crossing points and during the fixed opening hours'. Any new rules would need to apply to the long stretches of territory in between BCPs. This is no small order: these rules would have to cover threats to coastal borders and land. And they probably would need to take better account of unusual territorial entities – Spanish exclaves in North Africa; the border with British military bases in Cyprus; demilitarised islands in the Baltic; Mount Athos in Greece.

Fragmented: abolishing silos

The second great vulnerability comes down to the fact that Schengen is not the only regime for regulating the EU's borders. The EU in fact has three quite distinct border regimes, each covering a slightly different set of states and managed by a different set of authorities. Schengen is about regulating flows of people and is guarded by Frontex. But there is also a regime for goods flows. And the EU is increasingly active in getting military personnel and assets across NATO borders. Each border regime is the product of member states agreeing to make their shared borders more porous to flows of certain items and trying to guard a common outer border. But this leaves a legacy of coordination problems between immigration, customs and military services.

Hybrid attacks typically require a coordinated response from multiple different authorities. A hybrid attack on a border will pose a particular challenge, given that most governments rely on as many as 20 agencies to manage cross-border flows.[7] One might nevertheless think EU members were well-primed for this. As long ago as 2004 the EU began working towards a model of 'Integrated Border Management', so-called precisely because it would integrate the work of different border agencies. But, in fact, IBM is a product specifically of the Schengen regime, and the EU's 'integrated' approach to borders only really deals with flows of travellers and migrants. European customs authorities have developed their own distinct border model for goods flows, and they have begun integrating their work with Schengen authorities only because lorries now smuggle in human cargos alongside their usual contraband cigarettes and pharmaceuticals. As for the military, the Schengen IBM model more or less banishes soldiers from day-to-day border tasks.

A hybrid attack on a border will pose a particular challenge, given that most governments rely on as many as 20 agencies to manage cross-border flows.

In consequence Frontex, the EU's lead agency for borders, still struggles to cooperate with Europe's customs and military authorities. Frontex barely works with the EU anti-fraud office (OLAF) - the closest thing the EU has to a customs agency. Moreover both bodies have only lately begun to work with NATO, spurred by the Alliance's activities to control smuggling in the Aegean and Central Mediterranean. This lack of coordination is a vulnerability. Imagine the following scenario. At the border of the EU there is an acute influx of 'mixed' migration (irregular migrants, terrorists, foreign agents). A member state dispatches military assets to help. But getting its personnel and equipment across the EU is laborious because the Customs Union does not properly cover the flow of military assets. And when these do reach the border, these assets will also struggle to plug into

7 Martijn Pluim and Martin Hoffmann, "Integrated Border Management and Development", *ICMPD Working Paper*, no. 8 (2015), p. 12.

Frontex, which again operates under a different set of rules.[8]

Hostile third parties may exploit this fragmentation, devising a hybrid attack precisely to probe the EU's coordination problems and test the limits of solidarity in the EU. After all, when a member state suffers an acute border crisis, the EU expects its governments to show solidarity with each other by working across boundaries and silos. Article 222 of the Lisbon Treaty, the Solidarity Clause, requires the member states and the EU to use every tool at their disposal to respond to a man-made disaster. Similarly, the EU's Civil Protection Mechanism (CPM) foresees a mixing and matching of civilian and military resources. Back in the Cold War, the existence of a strong mutual solidarity clause – NATO's Article 5 – acted as a deterrent to the Soviet Union. So credible was the notion of collective defence, Moscow never actually tested it. The EU's current solidarity mechanisms, by contrast, are a plump target.

Only now is the EU integrating its three different border regimes – Schengen, customs and military. This is partly a response to the 2015 migration crisis, when Russia did indeed try to exploit Europe's fragmentation and directed migration flows at three countries in particular – Norway, Finland and Turkey. Had any of the trio called for solidarity in response to Russia's border actions, other European states would have found it hard to devise a comprehensive policy. After all, each of the three countries stands out in border terms. Finland is outside NATO, Norway is outside the Customs Union and Turkey is not party to Schengen. To achieve greater solidarity, the EU has now begun streamlining relevant financial instruments. Under the proposed MFF, customs authorities will be eligible for IBM-related funds, and military technologies with clear applications for customs and migration control will be funded.[9] Moreover, some funds are being made accessible to EU and non-EU members alike.

Blurred: sharpening EU border diplomacy

Countries can only really control their borders by cooperating with their neighbours. The EU has set the global standard for this kind of cooperation. Schengen members cooperate intensively with each other to lift passport controls. And they secure their shared outer border by cooperating with nearby Eastern European and North African countries. The EU expects Moldova, Ukraine and Morocco to help guard the Schengen border, and by way of reward it offers their citizens new travel opportunities to the Schengen Area. But this blurring of responsibility, and a recent crisis of faith in the EU's standards, has led to vulnerabilities.

The EU's mode of cooperating with third countries is being perceived more negatively. Russian analysts argue that this is a source of instability in the East. The EU uses measures such as visa facilitation to spread its home affairs rules. This is part of a long-standing commitment to 'people-to-people contact' with neighbouring third countries like Ukraine. Some Russian analysts trace upheavals like the Orange Revolution of 2004 to this approach. They say EU members waved through thousands of Ukrainian visa applications, leading to an uncontrollable circulation of people transmitting alien social and cultural values. In Russian eyes, such actions amount to hybrid warfare and apparently justify Russian hybrid campaigns in the West. It is not unusual to see Russian analysts point to the EU's visa-free policies towards Moldova and Ukraine as setting a precedent for Moscow's aggressive 'passportisation' in Georgia.

8 For their part, the member states are reluctant to share with Frontex information about how they would deploy their militaries in border contingency situations.

9 In really tricky spheres such as intelligence-sharing, too, there are signs that the military, customs and immigration services will be integrated. In 2018, for instance, the EU set up a 'crime information cell' on the flagship vessel of EUNAVFOR Med, bringing together the military, Frontex (on irregular migration) and Europol (on arms smuggling, terrorism and people smuggling).

When the EU exported its border rules, moreover, it also exported its own internal problems with coordination. The EU has long struggled to coordinate its immigration authorities with customs and the military, and this weakness now has international implications. The EU has, for instance, exported its Schengen border model to Eastern neighbours like Ukraine and Georgia. There are fears that this is not properly attuned to military threats. Following the Russian incursions of 2014, Ukrainian authorities were left to regret replacing their military model with an EU-style civilian one. Meanwhile, the EU cooperates with Balkan and African states to create a common assessment of immigration threats. This is useful for Frontex, but it may create problems for EU customs authorities. Some African and Balkan governments have links to criminals and terrorists. European customs officials worry that, by sharing its risk methodology, the EU will reveal its own border vulnerabilities.

Other standard-setting organisations like the OSCE and Interpol are becoming more influential in consequence. The sight of terrorists leaving Schengen territory to fight in Syria and of migrants flooding into Europe has dented the EU's reputation. But these other organisations are in turn being steered by wealthy backers. Interpol famously accepted a large donation from Philip Morris International, which wished to draw attention to cigarette smuggling. And the OSCE has allowed Russia to take the lead on problems such as human trafficking – issues seemingly designed to paint the EU in a bad light.[10] OSCE also receives large financial contributions from its Central Asian members. They stand accused of using border controls to crack down on the region's dissidents and of equating political dissent with terrorism. The EU is party to these organisations, and may face pressure to take on their new standards.

The EU's response to this politicisation of its border standards has been to build up links between frontline professionals. The aim is to ensure border issues are handled between peers on each side of the border, thus preventing disputes reaching the political level. This replicates the kind of approach traditionally adopted by the Finnish border service with its Russian neighbour. Russian and Finnish border guards meet regularly in joint committees, and their border posts are directly connected via a telephone hotline. Bulgaria recently followed the Finnish lead when it set up a 'fusion centre' with Greek and Turkish counterparts. This came in the wake of the arrest by Turkish authorities of Greek border guards who had wandered across the border. The arrest was politically motivated: Ankara offered to release the border guards if Athens handed over Turkish military officers who were seeking asylum in the EU.

Top-down: regulating people power

Schengen was created in order make the EU more relevant to its citizens. But its encouragement to people to link up across borders has a dark side. The EU is now dealing with a shadow human intelligence – irregular migrants and criminals sharing tips, for instance, and launching joint manoeuvres on the EU's border gaps. The problem is lent urgency by the fact that this collective human intelligence can be exploited by outside powers. New EU initiatives focus on regulating people power.

A new kind of criminal 'people power' is emerging in the EU. The 2008 financial crisis led to recruitment problems in national border and police services; widespread collusion between criminals and white collar professionals such as lawyers; a lowering of moral standards among EU citizens who are happy to consume cheap smuggled cigarettes and counterfeit pharmaceuticals; and the emergence of NGOs which are taking on roles recently vacated by the state, including border security and search and rescue. Europol's last two Serious and Organised Crime Threat Assessments (the 2013 and 2017 SOCTAs) highlight this trend. These reports

10 Moscow apparently loses no opportunity to paint the EU as a cesspit which draws Russian women into prostitution.

also show how the financial crisis exacerbated existing vulnerabilities: the government decisions in the 1990s to put military technologies in the public domain, and which today allow criminals and terrorists to organise themselves; technological breakthroughs in fields such as 3D printing which allow for the home production of counterfeit pharmaceuticals and drugs; the Snowden scandal which encouraged even ordinary citizens to use secure communications channels.

EU market integration has had the unfortunate effect of Europeanising organised crime. Traditional national mafias, with their hierarchies and codes of honour, are being replaced by pragmatic European networks of criminals, who sell highly-technical services, such as the counterfeiting of documents, and cheerfully cooperate with religious and political terrorists. They capitalise on their multi-ethnic mix, and they thrive in overcoming market barriers and national borders. They have adapted too to the EU's economy of scale, counterfeiting documents and money to meet continent-wide standards. And they pre-empt law-enforcement initiatives by carefully watching legislative processes in the European Parliament, as well as leak websites. Meanwhile licit firms like Facebook, Amazon, and travel agency Amadeo which benefit hugely from the single market are not always ready to pass useful information onto the EU.

The EU's border controls have proven vulnerable to this kind of collective human intelligence. 'Smart' borders are seldom that, at least not when faced with collaborative networks of criminals and migrants. The EU's web of border databases can be gamed. EURODAC, which stores asylum-seekers' fingerprints, is a case in point. The way the EURODAC system categorises entries has actively incentivised both migrants and border guards to abuse the system.[11] Fixing such problems has been a major endeavour of the EU's 'Security Union' agenda. It is closing gaps such as the absence of entry checks on EU citizens and of exit checks on visa holders. But the new systems are vulnerable, not least to disinformation efforts. The EU has chosen, for instance, to create the **European Travel Information and Authorisation System** (ETIAS), an advanced traveller information system rather like the American Electronic System for Travel Authorisation (ESTA). For citizens in the Western Balkans this entails new costs, and this has been picked up by critics of the EU in the region.

The member states' response has been to emphasise the value of HUMINT – that is, the intelligence gathered and deployed by border personnel on the ground. Take the controversy over Local Border Traffic Agreement (LBTA) documents. These documents which permit Ukrainians or Moldovans living in proximity to the EU border to cross easily are forgeable. Frontex frequently warns of the risk that terrorists and irregular migrants will take advantage of this fact. But there have not been any real problems: border guards are rooted in their locality and they know their regular travellers. As Frontex looks set to grow into a force of 10,000, member states are scrambling to retain a strong base of guards who know their particular stretch of member state border.

LESSONS: THE EU AS ITS OWN WORST ENEMY

On 19 November 2018, the EU held a border crisis preparedness exercise. The scenario was typical of many table-top exercises: it involved a high-intensity incident – an explosion at the border, a cyberattack which cripples a customs system, a hijacked cruise liner. These exercises serve to concentrate the minds of participants and have the benefit of being over in a few

11 Brigitta Kuster and Vassilis Tsianos, "How to Liquefy a Body on the Move: Eurodac and the Making of the European Digital Border" in *EU Borders and Shifting Internal Security*, eds. Raphael Bossong and Helena Carrapico (Cham: Springer, 2016), pp. 45-53.

hours. More probable in the real world, however, is a campaign of slow attrition through multiple hybrid events. It is precisely in this protracted situation, and with a lack of clarity on who is to blame, that the EU's own strengths may erode. There is a danger that intelligence analysts, who are used to thinking in terms of classic migration 'push' and 'pull' factors, will overreact and see malign forces everywhere facilitating migration and smuggling.

In the EU-28, light-touch borders are key to the economy and to diplomatic relations. Get the analysis wrong, and the costs are huge. The US offers an object lesson in this regard. In 1973, General Leonard Chapman retired from his command of the US Marines and took over the Immigration and Naturalization Service. Chapman had recently returned from serving in Vietnam, where the Marines had been in control of securing the line with North Vietnam. Having witnessed the effects of a border insurgency, he led a campaign to raise public awareness of the threat to the US and to militarise the US-Mexico border. This border had in fact been characterised by circular migration – by Mexicans passing into the US and out again shortly afterwards - but now became impassable to seasonal workers. Today, his experience serves as a lesson about a flawed threat perception and heavy-booted approach to a delicate border ecosystem.[12]

For the past two decades, the EU has made money from reducing border controls. The WTO helped it reduce non-tariff barriers such as customs checks and border waiting times. The resulting growth in cross-border trade more than offset the loss of import taxes to European coffers. But Frontex's new border technologies are costly. Even costlier is the need to help EU members which spent 20 years reducing their border services build them back up again. It is hard to see how these costs will be recouped. Business travellers are accustomed to travelling freely, and will not enjoy paying for trusted traveller status just to avoid bureaucratic hurdles which did not previously exist. The EU has already been forced to lower the price it charges for ETIAS in the face of discontent in the Western Balkans. It is precisely this kind of costly overreaction to border threats that the EU's rivals would be delighted to see.

In short, border guards have a delicate line to tread.

12 Chapman's story is widely used as a fable about the perils of heavy-handed border control. See for instance: Malcolm Gladwell, "General Chapman's Last Stand," *Revisionist History Podcast*, June, 2018, http://revisionisthistory.com/episodes/25-general-chapman%27s-last-stand

CHAPTER 2

NUTS AND BOLTS

Safeguarding the critical infrastructure of the Union

Energy pipelines, ports, railways, digital networks, undersea cables, space, power supply, banking and finance, food and public health and public services. These connectors and supply chains are the fundamental basis for the proper functioning of society and the economy. Critical infrastructure is, however, an inherently vulnerable aspect of economic and political life. Different forms of infrastructure are intertwined – think about how telecommunications networks support both government services and our ability to surf the web. In fact, the digitalisation of many traditional forms of infrastructure (energy, transportation, public services) opens up further vulnerabilities. To purposefully exaggerate for effect, whole supply networks can potentially be disrupted by the click of a button. Protecting critical infrastructure is also challenging because of the necessary interaction between different public and private actors that are responsible for the management of infrastructural services – this does not make policy coordination any easier. Furthermore, critical infrastructure is particularly vulnerable because of the EU's economic model which relies on global trade. Interdependence brings clear economic benefits, but it may also result in vulnerabilities. A zero inventory and just-in-time approach to supply ensures that even minor disruptions to supply chains can have serious knock-on effects for the rest of the economy and society.

It is no wonder, therefore, that critical infrastructure stands out as a particular target for adversaries looking to launch a hybrid attack against the EU. Physical and virtual networks and nodes offer an effective means by which to potentially paralyse whole societies. Furthermore, disrupting critical infrastructure can come with high deniability and non-military assets can be used to devastating effect. The cyberattack that partially shut down Estonia's communications networks and government institutions in 2007 is a good example. In this particular instance all eyes were on Moscow, but it is also the case that criminal networks are trying to exploit vulnerabilities in Europe's infrastructure to their advantage. It is commonplace for criminal networks to increasingly use malware to exploit mobile banking services, for example. Differentiating between state-sponsored and non-state attacks is a challenge and this makes all the difference when governments and/or institutions are looking for a potential hybrid campaign that might be escalated to a conventional conflict.

DISENTANGLING CRITICAL INFRASTRUCTURE NETWORKS

The protection of critical infrastructure has taken on a virtual and physical dimension. No longer can the EU and its member states focus simply on physical infrastructure protection (energy and transportation linkages). Indeed, virtual digital networks and infrastructure (5G networks) are just as important when

developing critical infrastructure protection strategies. Even more challenging, perhaps, is understanding how physical and virtual infrastructure networks are combined and why this fusion is relevant from a hybrid threats perspective. Unfortunately, there are plenty of examples of how virtual-physical infrastructures can be used to potentially devastating effect. For example, in March 2019 an aluminium plant in Norway experienced a ransomware attack that momentarily disabled smelting activities and risked overriding protection mechanisms. Back in May 2017, a number of hospitals in the United Kingdom had to cancel non-urgent operations and close certain wards because of a cyberattack. Finally, at the end of 2012 an electricity grid operator in Germany was subjected to a Denial of Service (DoS) attack aimed at freezing its access to networks – fortunately, this attack did not lead to any disruption to power transmission (see Figure 3 on page 26 for more information on the EU's key infrastructure linkages).

Another challenge associated with protecting critical infrastructure is how 'critical infrastructure' is even defined. For example, one can focus the definition on the protection of networks such as railway lines or energy pipelines and/or infrastructure nodes such as power stations or harbours. However, it is necessary to move beyond this basic understanding. Indeed, not only should digital infrastructure such as cyber networks be firmly included in any definition of critical infrastructure, but supply networks and chains should be classified as critical infrastructure too. This means that any comprehensive strategy to counter hybrid threats must consider how disruptions to the supply of medicine, food supply, raw materials and technologies can lead to the destabilisation of societies across Europe. Take, for example, the financial sector – it manages billions of euros worth of investments each day. One study from the International Monetary Fund (IMF) estimates that in 2015 the financial sector was the largest victim of cyberattacks and data breaches with close to 800 breaches in that single year – more than 90% of these cyberattacks emanated from unknown sources.[1]

The financial sector was the largest victim of cyberattacks and data breaches with close to 800 breaches in that single year.

In addition, the use of infrastructure networks to transport or operationalise CBRN devices and/or attacks should not be discounted (e.g. the nerve agent attack in Salisbury) and CBRN is accordingly a central pillar of the EU's response to hybrid threats.[2] Given the EU's essential maritime characteristics, maritime hybrid threats should not be discounted either. The littoral environment is congested and it is home to various maritime users, and so port security, maritime safety and the protection of undersea cables is essential. It should not be forgotten that 'little blue sailors' and coastguards can be used to forward state interests in the maritime domain under the threshold of military forces. In fact, in addition to improving situational awareness for both CBRN and maritime threats EU member states have launched specific projects under PESCO[3] and the EDF[4] to ensure that the Union has the physical capacity to respond to hybrid threats. In this respect, a 'system of systems' approach to infrastructure protection that considers the interdependency

1 Emanuel Kopp, Lincoln Kaffenberger and Christopher Wilson, "Cyber Risk, Market Failures and Financial Stability", *IMF Working Paper*, WP/17/185, 2017, p. 3.

2 European Commission, "Communication on a New Approach to the Detection and Mitigation of CBRN-E Risks", *COM(2014) 247 final*, Brussels, May 5, 2014, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/explosives/docs/20140505_detection_and_mitigation_of_cbrn-e_risks_at_eu_level_en.pdf

3 For example, the Harbour and Maritime Surveillance and Protection (HAMSPRO) project is designed to improve situational awareness in a maritime environment (the project involves three participating PESCO member states). There is also a specific project on 'CBRN Surveillance as a Service' (involving five participating PESCO member states).

4 For example, the Open Cooperation for European Maritime Awareness (OCEAN2020) project has been funded under the Preparatory Action on Defence Research (PADR) and €80 million has been earmarked for CBRN threat detection capabilities and counter drone systems under the European Defence Industrial Development Programme (EDIDP).

of physical and virtual networks and nodes, plus develops the capabilities needed to improve situational awareness and response, is required.[5]

The use of commercially available, sophisticated technologies such as drones has not made combatting potential hybrid threats any easier. Such technologies can be used to disrupt transport nodes, for example. As was the case at Gatwick (2018) and Heathrow (2019) airports recently, drones can be used to ground flights and cause havoc in Europe's air traffic management networks – more than 1,000 flights were affected by these two drone incidents alone. The European Aviation Safety Agency's (EASA) 'Drone Collision' task force estimates that drone incidents such as sightings over airports or near or actual collisions with aircraft have been on the rise since records began in 2010. While the data is incomplete and subject to interpretation, the EASA nevertheless estimate that there was a 1,150% increase in drone incidents from 2010 to 2016 and there was a notable spike in incidents in 2015 (a total of 500 individual incidents were reported).[6]

More than 1,000 flights were affected by these two drone incidents alone.

Democratic processes are also considered to be critical infrastructure. Ensuring that elections remain fair and free by rooting out harmful disinformation campaigns, data breaches or disruptions to electoral procedures is part of the critical infrastructure protection conversation now. This threat has taken on particular salience given the European Parliament elections in May 2019, but also because of evidence and/or reports of external interference in elections and referenda held in France (2017), Germany (2017), Netherlands (2014, 2016 and 2017), Spain (2017), the UK (2016) and the US (2016).[7] While a number of European countries do not permit electronic voting during national elections (e.g. Finland, Germany, Ireland, Lithuania, Netherlands, Spain and the UK), there are many facets to ensuring that elections are fair and free, including: the scrutiny of party funding, candidates and campaigns; cybersecurity for voting devices and procedures; and data protection. In this regard, the case of Cambridge Analytica's role in collecting and using data to help sway elections has given serious pause for thought. Of course, ascertaining which states, groups or individuals are behind election meddling is difficult as elections may fall prey to extremist groups, terrorist organisations and Eurosceptic movements and not just state actors. Nevertheless, there is evidence that shows that Russian-linked groups such as 'ATP28' (also known as 'Tsar Team' or 'Fancy Bear') are geared to undermining elections through the use of cyber espionage.[8]

The protection of EU institutions and processes should also be considered an essential part of any EU counter hybrid strategy. Not only are the EU institutions home to sensitive data but they play a critical role in managing the Single Market and key infrastructure in the European economy. In this respect, the EU institutions could be subjected to hybrid attacks and this implies that institutions need to have in place measures designed to ensure the resilience of EU networks and systems. This is a point referred to in the EU's Joint Framework on Countering Hybrid Threats and the attendant 'EU Hybrid Playbook' that is designed to

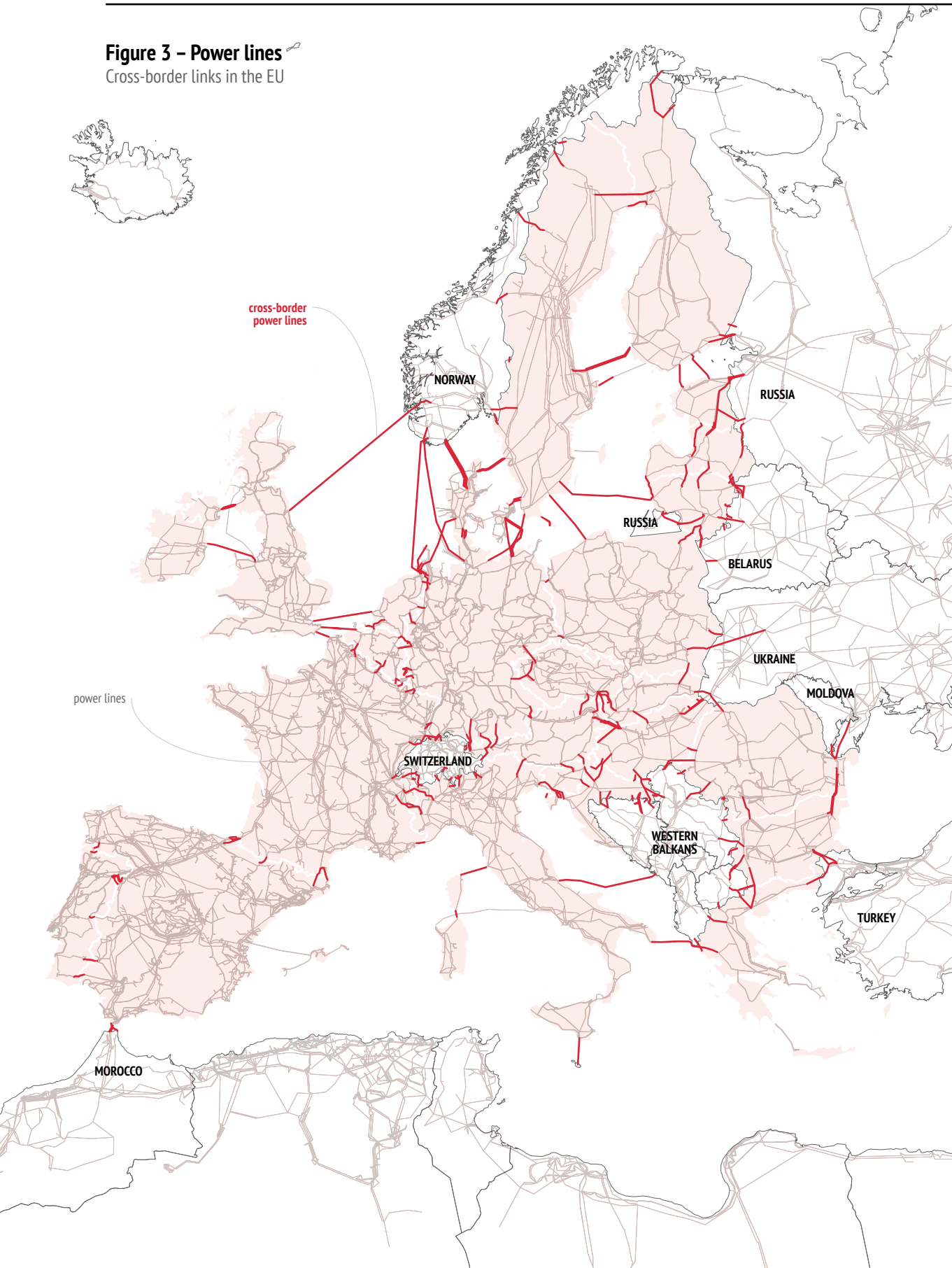
5 Frédéric Petit, Duane Verner, Julia Phillips and Lawrence Paul Lewis, "Critical Infrastructure Protection and Resilience – Integrating Interdependencies", in *Security by Design: Innovative Perspectives on Complex Problems*, ed. Anthony J. Masys (Berlin: Springer, 2018): pp. 193-219.

6 European Aviation Safety Agency, "'Drone Collision' Task Force", *Final Report*, October 4, 2016, https://www.easa.europa.eu/sites/default/files/dfu/TF%20Drone%20Collision_Report%20for%20Publication%20%28005%29.pdf, pp. 6-7.

7 Susan Davis, "Russia Meddling in Elections and Referenda in the Alliance", *General Report of the Science and Technology Committee*, NATO Parliamentary Assembly, November 18, 2018, https://www.nato-pa.int/download-file?filename=sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf, pp. 4-10.

8 EU Cybersecurity Agency, "ENISA Threat Landscape Report 2018", January 28, 2019, p. 112, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Figure 3 – Power lines
Cross-border links in the EU



structure and coordinate the EU's crisis response measures in case of a hybrid threat. This is not just important because the EU institutions may become a target for a hybrid campaign, but also because in the event of a hybrid attack leading to an invocation of the Solidarity Clause (Article 222 TFEU) by a member state, the EU institutions are supposed to be in a position to respond. Paralysed institutions could be challenged to fulfil this role.

Finally, any discussion of critical infrastructure protection must consider sensitive geopolitical questions and factors. At stake is the issue about ownership of critical infrastructure. The EU is an open economy but this can lead to harmful forms of FDI. This can range from land purchases near strategic infrastructure sites to purchasing controlling stakes in EU-based firms. 'Dummy firms' or sophisticated investment vehicles can be used by adversaries to either directly take control of infrastructure assets or use proxy firms to ensure this control. Obviously, in a hybrid context the ownership of critical infrastructure can raise a host of legal and security challenges. Recent data highlights that from 2009 to 2017 a total of 48 large investments in the EU gas and electricity sector were made by non-EU member states such as China (16 operations), US (8), Canada (8), Australia (5) and Russia (4).[9] There has, of course, been a long-standing concern about Russian ownership of or stakes in energy firms and supply networks, but the more recent case of Huawei's development of 5G networks in the EU and the suspected links between this company and the Chinese state has heightened European concerns. It is for these reasons that the EU developed its investment screening strategy in February 2019, which is designed not only to lead to increased information sharing between member states but to support those member states that seek to adopt a minimum set of requirements at the national level.

From 2009 to 2017 a total of 48 large investments in the EU gas and electricity sector were made.

THE EU AND CRITICAL INFRASTRUCTURE PROTECTION: THE STORY SO FAR

There are, therefore, multiple risks facing the EU's critical infrastructure but the fact that threats can arise in various sectors raises a particular challenge. Accordingly, it is difficult to ascertain whether risks in say energy infrastructure are linked to threats in public health. When confronted with multiple threats like this, the major test is to be able to prove with some degree of certainty that the combination of threats facing the EU in any given moment amounts to a hybrid campaign involving an external actor. In other words, when is a disruption to the EU's food supply simply a case of negligence or criminal behaviour and when does it become part of a hybrid campaign? The difficulty of answering this question might be a reason why the EU has taken a more preventative approach to critical infrastructure protection. This means that the EU is working to ensure that vulnerabilities are identified and remedied before they can be exploited by an external actor.

Although the EU has recently intensified its efforts to ensure critical infrastructure protection, there is a longer history to the Union's work in this area. Back in 2006, the European Commission published a Communication for a European Programme on Critical Infrastructure

9 See the Executive Summary of Milieu Ltd and E&A Law, "Review of National Rules for the Protection of Infrastructure Relevant for Security of Supply", *Final Report for the European Commission*, February 2018, https://ec.europa.eu/energy/sites/ener/files/documents/final_report_on_study_on_national_rules_for_protection_of_infrastructure_relevant_for_security_of_supply.pdf.

Protection (EPCIP) following being tasked to do so after the March 2004 European Council. Back then, the main concern for European leaders was the risk of a terrorist attack on European critical infrastructure rather than hybrid threats, especially following the terror attack in Madrid, Spain, on 11 March 2004. On this basis, the Commission set out a three-pronged approach to critical infrastructure protection: mapping of infrastructure in the EU, designing early warning mechanisms such as the Critical Infrastructure Warning and Information Network (CIWIN) and creating expert groups. The specific policy responses set out in the Communication were an admission that, owing to member state sensitivities about issues surrounding critical infrastructure, the EU did not have a clear idea of where vulnerabilities in cross-border infrastructure existed. Understanding that member state governments would remain hesitant about sharing information on their national critical infrastructure protection strategies, the Commission focused on cross-border infrastructure linkages with a special emphasis on risks that might spill over across the EU and/or from external states into the Union. In this respect, the Commission recognised that threats to critical infrastructure can emerge from man-made risks, technologies and/or natural disasters.[10]

The Communication was followed by a Council Directive in 2008 that focused on the identification and assessment of critical infrastructure in the EU. Member state governments recognised that even a rudimentary EU early warning network was required for cross-border vulnerabilities – by 'cross-border' the EU means a threat that affects two or more EU member states. One of the results of the Directive was to define what the EU meant when it spoke of critical infrastructure. In this respect, Article 2(a) of the Directive states that critical infrastructure is 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.[11]

Based on this definition, the Directive calls on EU member states to ensure minimum common standards for infrastructure protection. In order to achieve this, the Directive requests that basic information on national protection measures be shared between the member states and communicated to the Commission. Despite the fact that the exchange of information between member states on critical infrastructure is a notoriously sensitive issue, the Directive called on each member state to appoint 'Security Liaison Officers' (SLOs) as a basis for information exchange. What the Directive did not do, however, was specify what information should be exchanged by member states. National governments are reluctant to share their plans on critical infrastructure protection for various reasons, including the risk that national vulnerabilities will be exposed and that shared information may be leaked to third parties. Beyond the sensitivities surrounding information exchange, however, it should also be recognised that the Directive only covered energy and transport infrastructure and it did not refer to digital networks, space assets or the financial sector. It is for this reason that the Directive is currently being evaluated by the European Commission.

In lieu of a revised Directive for critical infrastructure protection, the EU has developed other steps and work strands to ensure that vulnerabilities in the EU's supply networks are identified and resolved. Accordingly, the EU has been keen to develop sectoral or thematic strategies in areas such as cybersecurity, energy security, maritime security and space, plus the Union has developed overarching

10 European Commission, "Communication on a European Programme for Critical Infrastructure Protection", *COM(2006) 786 final*, Brussels, December 12, 2006, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

11 Council of the EU, "Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection", *2008/114/EC*, Brussels, December 8, 2008, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

strategies specifically focused on countering hybrid threats. Even though the obvious question is whether the EU can ensure coherence for all these individual initiatives, each one has attempted to think about longstanding issues such as critical infrastructure protection from a hybrid threats perspective. Before soon turning to the Union's overarching hybrid threat strategies, it is worth looking at some of the specific initiatives developed by the EU in more detail.

Cybersecurity

The EU's 2013 Cybersecurity Strategy attempted to stress the importance of virtual critical infrastructure in addition to physical infrastructure. The cybersecurity strategy points to similar measures already addressed in the 2008 Directive on physical critical infrastructure, as can be seen by the language on cyber information-sharing and capacity building in the member states. Yet, the cybersecurity strategy is notable in at least two important respects: it places much more emphasis on involving the private sector in responses to potential critical infrastructure threats, and it links cybersecurity with the EU's external action and security and defence policies (a noteworthy move given the external dimension of hybrid threats).[12] Crucially, the EU built on the cybersecurity strategy by agreeing to a specific Directive on security of network and information systems, which was adopted in July 2016. The Directive put into EU soft law the requirement that member states: (i) appoint a Computer Security Incident Response Team (CSIRT) or national authority to respond to cybersecurity incidents; (ii) engage in a coordination network (the 'CSIRT Network') for the purposes of information sharing; (iii) ensure that essential services and suppliers have appropriate security measures in place and that they report serious cybersecurity incidents to national authorities.[13]

Furthermore, cybersecurity features as a crucial element of how the EU plans to protect its digital networks. For example, on 26 March 2019 the Commission published a recommendation on the cybersecurity of 5G networks. Such networks will be vital for the maintenance and operation of energy, transport, banking, health, industrial and democratic infrastructure. The Commission call for 'European sovereignty' in 5G networks and it is made clear that China poses a risk in this regard because of Beijing's growing technological presence in the EU and its foreign investment in strategic sectors and critical infrastructure. The recommendation calls on EU member states to complete national cybersecurity risk assessments based on how national authorities certify digital products and services and in the way telecommunications networks are maintained. The assessments are due to be submitted to the Commission and the European Agency for Cybersecurity (ENISA) by 15 July 2019. On this basis, ENISA will then conduct a 5G threat and risk landscape assessment by 1 October 2019. One year after this date, the member states should decide on whether further action is required.[14]

Energy

The 2014 European Energy Security Strategy clearly builds on the 2008 Directive on critical infrastructure, too. The strategy again goes further than simply calling for greater coordination between member states by urging the member states to strengthen their emergency and solidarity mechanisms, and by coordinating risk assessments and contingency plans for

12 European Commission/High Representative of the EU for Foreign Affairs and Security Policy, "Joint Communication on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", *JOIN(2013) 1 final*, Brussels, February 7, 2013, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

13 European Parliament and Council of the EU, "Directive Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union", *(EU) 2016/1148*, Brussels, July 6, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

14 European Commission, "Commission Recommendation – Cybersecurity of 5G Networks', *C(2019) 2335 final*, Strasbourg, March 26, 2019, https://www.droit-technologie.org/wp-content/uploads/2019/03/reco.pdf

critical infrastructure protection. With the view to creating a fully-fledged internal market for energy, the strategy scratches well below the surface of the 2008 Directive by calling for coordinated response strategies to energy security issues and not just information sharing. Furthermore, the energy security strategy moves beyond the physical protection of infrastructure assets because it raises the important issue of company ownership. Perhaps as a noteworthy precursor to the EU's recent initiatives on FDI screening,[15] the energy security strategy states that EU strategic debates on energy 'should address the control of strategic infrastructure by non-EU entities, notably by state-companies, national banks or sovereign funds from key supplier countries, which aim at penetrating the EU energy market or hampering diversification rather than the development of the EU network and infrastructure'.[16]

This observation is particularly salient given the interest Russia continues to show in the EU energy market and the ongoing political debates about the planned construction of the Nord Stream 2 pipeline from Russia to Germany. Protection of European energy infrastructure is thus an economic and geopolitical issue. In this respect, the European Commission has developed a range of mechanisms designed to enhance the supply of gas, oil and electricity throughout the EU. Such initiatives centre on member state coordination through the Gas Coordination Group (GCG), the Oil Coordination Group (OCG) and the Electricity Coordination Group (ECG); diversification and maintaining emergency stocks of crude oil and petroleum products; and response networks such as the European Network for Transmission System Operators for Gas (ENTSOG) and the European Network of Transmission System Operators for Electricity (ENTSO-E).

Maritime

Much like the energy security strategy, the 2014 EU Maritime Security Strategy recognises that critical infrastructure protection is a vital component of the EU's overall security and defence. There is an obvious external dimension to maritime security in the EU because more than 70% of the Union's external borders are maritime and most EU trade is carried over the world's seas and oceans.[17] In outlining the EU's maritime strategy, the Council of the EU acknowledged that maritime threats may emerge out of cybersecurity and CBRN attacks, but, just like other strategies, it called for a shared risk analysis of maritime security, the 'stress testing' of critical infrastructure, preparation for possible Article 222 contingencies and information exchange. The Council has continued to focus its efforts on maritime security. Indeed, only a few months after the release of the maritime strategy the Council published an Action Plan in December 2014 to put the strategy into practice.[18] The Action Plan reiterated the need for shared risk analysis and management, especially for where two critical infrastructure domains meet (e.g. maritime protection of energy installations such as offshore platforms or undersea cables), and for greater R&D and innovation in maritime surveillance and protection technologies. Following the 2018 revision of the Action Plan, the Council explicitly referenced the challenge of hybrid threats but it also acknowledged that one of the tests facing the EU is to ensure 'better coordination' so that the multitude of initiatives and strategies developed by the EU on critical infrastructure protection make sense in the round.[19]

15 European Union, "Regulation Establishing a Framework for the Screening of Foreign Direct Investments into the Union", *2017/0224 (COD)*, Brussels, February 20, 2019.

16 European Commission, "Communication on a European Energy Security Strategy", *COM(2014) 330 final*, Brussels, May 28, 2014: p. 6, https://www.eesc.europa.eu/resources/docs/european-energy-security-strategy.pdf

17 Council of the EU, "European Union Maritime Security Strategy", *11205/14*, Brussels, June 24, 2014: p. 2.

18 Council of the EU, "EU Maritime Security Strategy (EUMSS) – Action Plan", *17002/14*, Brussels, December 16, 2014, http://data.consilium.europa.eu/doc/document/ST-17002-2014-INIT/en/pdf

19 Council of the EU, "Council Conclusions on the Revision of the EU Maritime Security Strategy (EUMSS) Action Plan (26 June 2018)", *10494/18*, Brussels, June 26, 2018, p. 4, http://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf

Space

The 2016 Space Strategy for Europe went much further than the 2008 Directive on critical infrastructure by stressing the need to protect the EU's space infrastructure. The space strategy is quite remarkable in that it clearly identifies potential vulnerabilities and it shows how space is vital for all other forms of critical infrastructure protection (e.g. transport, agriculture, maritime, telecommunications, energy, etc.). One of the strategies developed by the European Commission to ensure the security of the EU's space infrastructure is to ensure the commercial and public uptake of Galileo and Copernicus services. In this respect, the Commission understands that greater use of Galileo and Copernicus will ensure that the EU is not dependent on external global positioning systems (GPS). Yet greater autonomy is not the only way to protect space infrastructure. Indeed, the space strategy makes plain that a greater effort is required if satellites and systems are to be resilient to cyberattacks, space debris and abnormal space weather conditions.[20] It is for this reason that specialised teams (e.g. the Galileo Security Monitoring Centre (GSMC)) have been set up under Galileo to ensure the security of the system.

Overarching strategies

In addition to the specific strategies on cyber, energy, maritime and space security stand a number of overarching strategies that are geared to providing overall coherence for the EU's counter hybrid strategies. While the 2008 Directive on critical infrastructure feels slightly dated in the light of the shifting geopolitical and technological challenges facing the EU, the Union has published a number of communiqués that are designed to pull individual strategies together. These include the 2015 European Agenda on Security, the 2016 Global Strategy for the EU's Foreign and Security Policy, the 2016 Joint Framework for countering hybrid threats and the 2018 Joint Communication on resilience and hybrid threats. In particular, the European agenda and the global strategy are attempts to frame and respond to hybrid threats from an internal and external security perspective. Whereas the Agenda looks at the specific risk posed by criminal networks and terrorist organisations[21], the global strategy states that 'living up to the [EU's] commitments to mutual assistance and solidarity [...] includes addressing challenges with both an internal and external dimension, such as terrorism, hybrid threats, cyber and energy security, organised crime and external border management'.[22]

The specific initiatives on countering hybrid threats are worth reading from the perspective of critical infrastructure protection. The 2016 Joint Framework on Countering Hybrid Threats, for example, calls for member states to conduct a hybrid risk survey in order to better understand risks and vulnerabilities. In this respect, the Joint Framework adds to the energy and maritime security strategies by calling for a diversification of energy sources and greater protection and safety of electricity grids, nuclear infrastructure, transportation networks, maritime and space infrastructure, food and health supply chains, cyber networks and financial networks.[23] Despite such calls, however, it remains unclear to what degree the member states will be willing to conduct such a risk survey given the sensitivities surrounding information exchange. Nevertheless, the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid

20 European Commission, "Communication on a Space Strategy for Europe", *COM(2016) 705 final*, Brussels, October 26, 2016, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF

21 European Commission, "Communication on the European Agenda on Security", *COM(2015) 185 final*, Strasbourg, April 28, 2015, http://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf

22 High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission, *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the EU's Foreign and Security Policy*, June 2016, p. 20.

23 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on a Joint Framework on Countering Hybrid Threats", *JOIN(2016) 18 final*, Brussels, April 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

threats outlines specific initiatives that will enhance the EU's ability to respond to hybrid threats and critical infrastructure protection. For example, the Communication states that the Hybrid Fusion Cell created in the EEAS in 2016 to detect hybrid threats will from 2018 have a responsibility for counter-intelligence and CBRN too. In this respect, the Communication calls for greater national intelligence sharing so that the fusion cell may receive information on hybrid threats from the national hybrid points of contact (PoCs).

ENSURING THAT RESILIENCE BECOMES THE NORM

When one looks at the range of strategies and initiatives developed by the EU for critical infrastructure protection, it is apparent that common threads and logics are embedded in each one. The EU needs to be better at situational awareness and the member states need to exchange information on threats and vulnerabilities. Despite all the efforts to develop capabilities, networks of expertise and early warning systems on critical infrastructure protection, the main obstacle remains the continued reluctance of EU member states to consistently share quality intelligence with each other through the EU. This is a point that several iterations of the Commission's Security Union progress reports have stressed.[24] While failing to exchange information could itself be considered a vulnerability when it comes to securing cross-border infrastructure, there are understandable reasons why national governments and authorities remain hesitant to share information and risk analysis. Not only might it expose weaknesses in infrastructural protection measures and capacities, but such information might be inadvertently leaked to actual or potential adversaries that crave a more detailed picture of national vulnerabilities and response strategies to hybrid threats. Furthermore, sharing information at the EU level could be seen as empowering EU institutions at the expense of national authorities. For these and other reasons, infrastructure protection will remain a national competence for the foreseeable future.

This is not to suggest that the 'sovereignty card' has completely hampered EU efforts to improve information exchange. As the Joint Report on the implementation of the joint framework on countering hybrid threats makes clear, a manual of vulnerability indicators and resilience for hybrid threats to critical infrastructure is being developed by the European Commission and the member states are already part of a common risk assessment mechanism for security of gas and electricity supply. Similar mechanisms are being developed for nuclear security and cybersecurity.[25] Furthermore, within the Council of the EU the Friends of the Presidency Group (FoP) on hybrid threats has been coordinating surveys and assessments on key vulnerabilities to hybrid threats and its mandate up to 2020 (extended for a further two years in 2018) will ensure that this work continues. Therefore, the EU recognise that information sharing is key for critical infrastructure and hybrid threats. The question is whether the information being exchanged is useful and whether a common vulnerability assessment will lead to quality intelligence and situational awareness. The risk with common assessments is that they can potentially represent the lowest common denominator of information exchange.

Additionally, when thinking about critical infrastructure it is necessary to involve private actors and firms in response mechanisms. Private actors own full or partial stakes in key capacities which means that companies are on

24 See, for example, European Commission, "Eighteenth Progress Report towards an Effective and Genuine Security Union", *COM(2019) 145 final*, Brussels, March 20, 2019, p. 2, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190320_com-2019-145-security-union-update-18_en.pdf

25 European Commission, "Joint Report on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018", *JOIN(2018) 14 final*, Brussels, June 13, 2018.

the front line of protecting critical infrastructure. In a hybrid threats context, the risks here relate to how public and private actors interact with each other when designing protection and resilience measures, plus there is an obvious concern regarding which actors' own private companies in the EU (i.e. external actors owning shares in EU infrastructural assets). The interaction between public and private actors is especially vital in the cyber domain. The biggest challenge in protecting critical infrastructure is ensuring sound lines of communication between public authorities and private contractors. Governments and authorities can subcontract services to firms, but these firms may not have optimal cybersecurity measures, which in turn exposes a weakness in national resilience structures and mechanisms.[26]

Apart from ensuring coherence between public and private actors, however, is the challenge connected to the information asymmetry between companies and governments. In most areas of critical infrastructure protection, firms develop sophisticated technologies to protect their investments but these technologies may produce vulnerabilities that governments are slow to understand and/or regulate. This is particularly true when it comes to digital technologies and digital infrastructures (e.g. the development of algorithms and/or use of big data). Ensuring that private firms live up to their responsibilities with regard to security and hybrid threats is an essential component of critical infrastructure protection strategies, not least because firms can operate across borders in the single market and in certain cases they might be owned by non-EU investors with possible ulterior motives.[27] Lastly, without the involvement of the private sector it will be difficult for the EU to develop a meaningful common risk and vulnerability assessment mechanism for critical infrastructure protection. Such an assessment should have the buy-in from relevant firms as well as member state governments.

26 See, for example, Joseph Kramek's study of cybersecurity in the context of US port facilities. Joseph Kramek, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities", *Brookings Institute Policy Paper*, July 2013, https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf.

27 Jarno Limnéll, "Countering Hybrid Threats: Role of Private Sector Increasingly Important – Shared Responsibility Needed", *Strategic Analysis*, March 2018, European Centre of Excellence for Countering Hybrid Threats, p. 6, https://www.hybridcoe.fi/wp-content/uploads/2018/03/Strategic-Analysis-2018-3-Limnell.pdf.

CHAPTER 3

HEARTS AND MINDS

Enhancing societal resilience against disinformation

Do not believe the truth. Critical engagement with government policy and political issues is a prerequisite for a healthy democracy, but when trust in political institutions and processes is broken then disenchantment, antipathy and demagoguery can take hold. If a state or actor wanted to undermine the strength of a democratic or open society, then undermining the confidence of citizens in their political institutions and processes would be an obvious place to start. Spreading falsehoods and lies within a society can undermine institutions and this is an ideal way to prepare the ground for escalatory measures in a hybrid threat context. Disinformation can be understood as information that is verifiably false or at least misleading, and disinformation campaigns are designed to intentionally deceive the public. Successful disinformation campaigns can undermine electoral processes and can alter political debates, thereby altering the parameters or margin for manoeuvre for governments. In extreme cases, disinformation can be used to sow the seeds of division in society.

Twitter have also reported that they removed 3,613 Russia-related accounts in October 2018 and 416 more in January 2019.

Technologies and applications such as smart phones and social media have only increased and amplified the efficacy and penetration of disinformation campaigns. The sheer range and volume of information available on the internet means that there already exists a congested media and information environment. Multiple news sources exist and individual bloggers and new media sources can easily influence social groups and individuals. What is more, the use of social media and online news sources allows the perpetrators of fake news and disinformation to pursue their activities anonymously and at minimal cost. Internet trolls and sock puppets are able to spread false information and call the credibility of data sources and news reports into question. For example, one report submitted to the US Congress in 2017 estimates that approximately 80,000 pieces of Russian government-sponsored content reached 29 million people on Facebook between January 2015 and August 2017.[1] Twitter have also reported that they removed 3,613 Russia-related accounts in October 2018 and 416 more in January 2019, in addition to over 3,000 Iran-linked accounts since October 2018.[2] From a hybrid threats perspective, the anonymity and deniability that comes with online personas, spambots and dummy accounts provides a convenient and effective screen for hostile governments, terrorist networks and

1 Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 million through Facebook Alone", *New York Times*, October 30, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

2 Twitter, "Elections Integrity: We're Focused on Serving the Public Conversation", https://about.twitter.com/en_us/values/elections-integrity.html#data

extremist groups. The low cost of mobilising social media tools is also a contributing factor as to why disinformation has re-emerged as a popular tool for adversaries.

DEMYSTIFYING DISINFORMATION

The EU defines disinformation 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'.[3] In this regard, it is necessary to immediately distinguish between disinformation and more traditional forms of propaganda – although during the Cold War the Soviet Union managed to use disinformation as part of broader propaganda campaigns against the US and its allies. In contrast to disinformation, propaganda is usually associated with tactics and strategies that are designed to disseminate messages and views in support of a particular political cause, ideology or interest. Propaganda is designed to crack the morale of soldiers during wartime or to play on the ideological loyalties and leanings of academics, spies and public figures. Sowing disinformation is a way to foment distrust and antipathy in established practices and norms but for this reason it is no less nefarious than propaganda. Unlike propaganda, which is usually marked by bold advertising campaigns or covert intelligence work, disinformation is not so easy to detect and it has no discernible political cause or message. In many cases, there is also a fine line between disinformation and conspiracy theories.

More traditional forms of disinformation featured adversaries providing a counter argument to an idea or political doctrine or sowing falsehoods that unwitting media sources would spread to citizens. Disinformation rests on the potent idea that a counter narrative is reasonable and plausible. For example, the idea that the US military purposefully spread HIV/AIDS to Africa was spun by 'Department D' (D for *dezinformatsiya*) at the KGB under Operation Infektion, and the idea was to tarnish the US's image around the world and also exacerbate racial divisions in America. The message was widespread and effective because US news channels got a hold of the claim and broadcast it nationally – they managed to do the hard work for the Soviets. Another strategy employed by the KGB was to forge top secret letters purportedly from high-ranking American officials calling for the assassination of foreign leaders or military intervention. The forged letters were promulgated through media channels across the globe by irate citizens or groups reportedly coming across the secret letters by chance or mistake.[4] Again, such stories were planted in the mass media with the aim of disseminating a falsehood and ensuring that readers of the story would think it plausible. Importantly, all of these disinformation strategies were designed to not lead back to KGB operatives.

Similar strategies are used by Russia today in the wake of Moscow's illegal seizure of Crimea. In particular, pro-Kremlin or state controlled media have targeted NATO forces and allies. As the EEAS East StratCom Task Force's 'EU versus Disinformation' campaign shows, Russia has used official social media accounts to spread falsehoods about the level of troops deployed by NATO during military exercises. One tweet by the Russian Embassy in London from 3 November 2018 claimed that NATO had deployed 11,000 troops in Estonia, Latvia, Lithuania and Poland near the Russian border. Russia claimed that NATO was amassing troops on the border for an imminent invasion. This could not have been further from the truth. NATO had deployed only 5,000 troops and the detachment was part of the Alliance's reassurance measures in the wake of Russian aggression in the region. NATO

3 European Commission, "Communication on Tackling Online Disinformation: A European Approach", *COM(2018) 236 final*, Brussels, April 26, 2018, http://www.europarl.europa.eu/resources/library/media/20180926RES14426/20180926RES14426.pdf

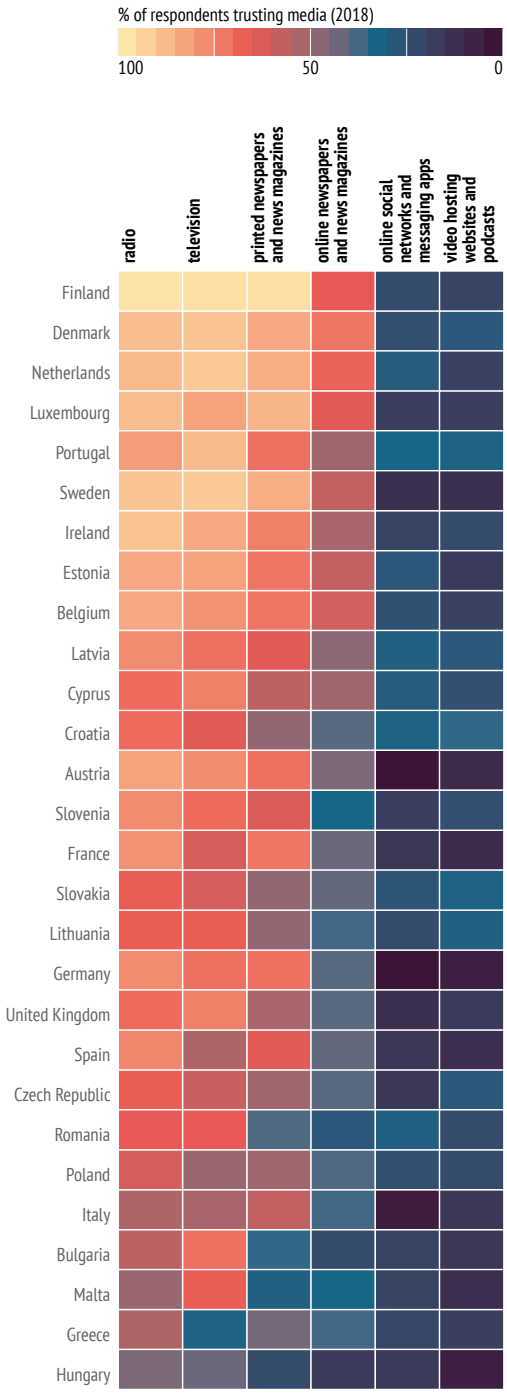
4 L. John Martin, "Disinformation: An Instrumentality in the Propaganda Arsenal", *Political Communication*, vol. 2, no. 1, 1982, pp. 47-64.

transparently and publicly disclosed the troops and equipment it had deployed on rotation to the region (and, incidentally, NATO territory). Russian disinformation campaigns have also claimed that NATO's Trident Juncture 2018 exercise was comparable to the Nazi invasion of Norway in 1940.[5] German soldiers that were stationed in Lithuania in 2017 were accused of raping an underage girl and the fake story was spread through various media outlets wile an email was sent to the Lithuanian parliament to further sow division.[6]

Despite these campaigns, however, there is a need to recognise the importance of how modern day disinformation campaigns are augmented by technologies and applications such as social media. The established theory is that social media is an effective way of spreading disinformation on a rapid and global basis. But the potency of social media and digital networks runs deeper than this. Academic studies focusing on how social media can affect consumer behaviour gives us an insight into how disinformation might work in the virtual world.[7] Consumers will indeed view an advert for a commodity, but they are unlikely to be influenced or convinced to buy the commodity at this stage. What is observed is that a consumer will attempt to corroborate the news item or opinion on a commodity by consulting online reviews, blogs, other social media (e.g. looking at photos about the commodity on Instagram) and talking to friends or family about it. In other words, consumers tend to seek out more information about a product and human validation is still important. This same logic carries over into disinformation in a hybrid threat context. The consumer of news or information is confronted with a provocative message or news item and they will then seek out more

Figure 4 – Media divides trust

People trust news and information from traditional media more than online media



Data: Eurobarometer, 2018

5 EU vs Disinformation, "'Funeral Teams for NATO Soldiers' – A Week of Disinformation Scare-Mongering, Exaggeration and Mockery", November 8, 2018, https://euvsdisinfo.eu/funeral-teams-for-nato-soldiers-a-week-of-disinformation-scare-mongering-exaggeration-and-mockery/

6 "NATO: Russia Targeted German Army with Fake News Campaign", *DW News*, February 16, 2017, https://www.dw.com/en/nato-russia-targeted-german-army-with-fake-news-campaign/a-37591978

7 See, for example, Andrew T Stephen, "The Role of Digital and Social Media Marketing in Consumer Behaviour", *Current Opinion in Psychology*, vol. 10, 2016, pp. 17–21.

information by consulting comments boxes, linking to other fake news accounts and speaking about the news to friends, colleagues and family. It is this process which determines how successful a disinformation campaign is.

Yet news and information consumption on social media needs to be put into some context because human behaviour and taste changes (see Figure 4 opposite). First, in a recent Eurobarometer poll 54% of citizens said they do not trust news or information accessed through online social networks and messaging apps.[8] Yet, evidence shows that consumers of news via social media platforms are also shifting their habits and behaviour. The use of platforms such as Facebook is on the decline in many Western countries, but sharing news media in select groups via messaging apps is on the rise. This can, of course, make tracing and refuting disinformation much harder. Messaging apps are encrypted and so intelligence and/or law enforcement is made much harder. Furthermore, news consumption is on the rise through podcasts and voice-activated digital assistants. The relevance and/or increased use of imaging services such as Instagram and Snapchat for news consumption should also not be discounted.[9] Shifting attitudes to social media networks play a key part in how disinformation campaigns can be promulgated and sustained.

In a recent Eurobarometer poll 54% of citizens said they do not trust news or information accessed through online social networks and messaging apps.

However, it is all too easy to point to social media as the sole reason for why disinformation campaigns are so potent today. First, traditional forms of media such as television, radio and newspapers still have substantial mass appeal and they bear a responsibility for spreading fake news. When popular news channels or newspapers seek only the revenue generated by followers, there is sometimes a temptation to willingly and unwittingly reproduce disinformation. The so-called 'click bait' culture may lead to better viewing figures, but it also contributes to an erosion of trust in public or reputable private media companies. In this respect, disinformation campaigns thrive on the 'legitimacy' that can be garnered from large news companies reproducing fake news. Not only does mainstream media endorsement make disinformation appear more credible, but the dissemination of mistruths and falsehoods will eventually be exposed and reporters (rather than the original creators of the disinformation campaign) can usually be held responsible by the public. Second, disinformation is unlikely to shift public behaviour on its own because complex psychological and ideological factors feed into why an individual would believe a piece of fake news. For example, deft disinformation campaigns will usually target the political sensibilities of audiences through the use of icons, images, political slogans and even social media identities and labels (e.g. Twitter handle names).[10]

8 Eurobarometer, "Flash Eurobarometer 464: Fake News and Disinformation Online", February 6, 2019, https://data.europa.eu/euodp/data/dataset/S2183_464_ENG

9 Nic Newman et al., "Reuters Institute Digital News Report 2018", *Digital News Report 2018*, 2018, http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475

10 John D. Gallacher and Rolf E. Fredheim, "Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home", in *Responding to Cognitive Security Challenges*, eds. Sebastian Bay et al (Riga: NATO StratCom Centre of Excellence, 2019), p. 76.

DEFLECTING AND REFUTING DISINFORMATION THE EU WAY

Given how disinformation campaigns are designed and deployed, and how individuals and groups engage with or are influenced by such campaigns, it is worthwhile reviewing how the EU has approached countering disinformation. The first step taken by the Union in the wake of Russia's seizure of Crimea was to develop Strategic Communication (StratCom) teams that were tasked with refuting disinformation sources. As the 2015 Action Plan on Strategic Communication observed, '[t]he use of communication tools has played an important role in the dramatic political, economic and security related developments that have affected the EU's eastern neighbourhood'.[11] In particular, in March 2015 the EU established the East StratCom Task Force in the EEAS with the aim of countering Russia disinformation. Since 2015, East StratCom has reported and refuted over 5,000 instances of disinformation on the Ukraine, US military, the migration crisis, Daesh, the Salisbury chemical weapons attack and the downing of flight MH17 in July 2014. Such disinformation was spread by Russian-based news operators or by Russian-backed sources operating in the EU. What is more, the Task Force has worked to design and disseminate positive strategic communications in the Eastern neighbourhood countries. The EU built on the early success of East StratCom by establishing two further task forces for the Southern neighbourhood and for the Western Balkans in 2017.

Since 2015, East StratCom has reported and refuted over 5,000 instances of disinformation.

Following on from the creation of the StratCom task forces, the European Commission published a Communication on tackling online disinformation in April 2018. The Communication sought to address the fears of member state governments that electoral processes could be influenced by disinformation campaigns (e.g. European Parliament elections in May 2019). The Commission rightly acknowledged that disinformation is a 'symptom of wider phenomena that affect societies facing rapid change' such as economic insecurity and extremism which can lead to polarisation, social tensions and distrust. It also observed that huge shifts in the media sector were underway with revenue streams shifting away from traditional media companies towards online news. This has not only resulted in unconventional media companies entering the market but it has also meant that established news companies alter their advertising and reporting models.[12]

To tackle disinformation, the Commission proposed a four-pronged strategy of: (i) enhancing transparency about the origin of information and how it is produced, sponsored and disseminated; (ii) supporting high quality journalism and media literacy with the aim of enhancing the diversity of information and critical thinking; (iii) enhancing the trustworthiness and credibility of information by working with key stakeholders; and (iv) boosting public awareness and media literacy.[13] On this basis, the Commission decided that it was time for an EU-wide Code of Practice on disinformation and it sought to create an independent network of European fact checkers, as well as engaging the academic community to help detect and respond to disinformation. Additionally, EU member states were also directly addressed by the Communication and the Commission called

11 European Union, "Action Plan on Strategic Communication", *Ref. Ares(2015)2608242*, Brussels, June 22, 2015, http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf.

12 European Commission, "Communication on Tackling Online Disinformation: A European Approach", *COM(2018) 236 final*, Brussels, April 26, 2018.

13 Ibid.

on governments to do more to aid quality journalism and provide training programmes on a national basis. A sound counter disinformation strategy has to involve local, regional and national governments and the media.

Following on from the Communication, the European Commission launched two concrete initiatives in September 2018. The first was the Code of Practice for disinformation, which called for the self-regulation of online social companies against disinformation along 11 points including: agreeing to scrutinise adverts that spread disinformation, ensuring transparency of political or issue-based advertising, closing fake accounts and disabling bots, promoting trustworthy content and working to ensure the high standards of data protection.[14] Ensuring that companies respond to disinformation on their sites is a key challenge, but the Code of Practice seeks to build on the changes that were already under way in the social media landscape. After all, social media companies already have legal obligations in many countries to counter and dissuade hate speech, gender-based and racial discrimination, cyber bullying, etc.[15] While there is evidence to suggest that social media companies have a market imperative to ensure reliable and safe online spaces,[16] the Commission adopted a strategy of self-regulation in order to ensure that a healthy balance between openness and regulation was struck.

The second concrete action taken by the Commission came in the form of the so-called 'Election Package'. The package was designed to look at data protection, the transparency of political advertising, cybersecurity and elections and the possible application of sanctions on European political parties and political foundations should they breach data protection rules in order to influence European elections. The backbone of the election package was a Commission Recommendation on how to secure fair and free elections. Member states were called upon to ensure the swift exchange of information and lessons learned with each other, and national authorities were asked to ensure that national systems of protection are bolstered. In particular, the Recommendation asked member state governments to enhance transparency in political advertising and funding through 'the active disclosure to citizens of the Union of information on the political party, political campaign or political support group behind paid online political advertisements and communications'.[17] What is more, the Commission made clear that cybersecurity was an indispensable part of ensuring fair and free elections and to this end it called for the full application of the NIS Directive and use of the NIS cooperation group to coordinate network protection strategies.

Following on from these two initiatives, the Commission and the HR/VP released a Joint Action Plan on Disinformation in December 2018. The Action Plan serves as another overarching strategy that reflects a joint Commission and EEAS understanding of disinformation. Furthermore, the plan recognised that the StratCom task force teams needed extra support and should be upgraded in light of evolving disinformation campaigns and strategies. The plan also reiterated the importance of the 'Election Package' and the Code of Practice, but it also stressed the need for the EU to intensify its strategic communication campaigns within the Union and the neighbourhood as well as to develop media literacy in the EU (e.g. through cross-border media initiatives

14 European Commission, "EU Code of Practice on Disinformation", September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

15 Jarno Limnell, "Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed", *Strategic Analysis*, March 2018, European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/wp-content/uploads/2018/03/Strategic-Analysis-2018-3-Limnell.pdf

16 Bertin Martens et al., "The Digital Transformation of News Media and the Rise of Disinformation and Fake News", *JRC Digital Economy Working Paper 2018-02*, Joint Research Centre Technical Reports, European Commission, April 2018; p. 47.

17 European Commission, "Recommendation on Election Cooperation Networks, Online Transparency, Protection Against Cybersecurity Incidents and Fighting Disinformation Campaigns in the Context of Elections to the European Parliament", *C(2018) 5949 final*, Brussels, September 12, 2018, p. 8, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

and a Media Literacy Week). Of course, one of the chief drivers of the Action Plan was the European Parliament elections in May 2019, but the Commission and HR/VP made clear that the plan would also support presidential, national and local-regional elections in the member states – more than 50 such elections are to be held in the EU by 2020.[18]

However, one of the other concrete proposals that the Action Plan outlined was the need to create a Rapid Alert System (RAS) for disinformation so as to enhance exchange of information on disinformation between the member states and EU institutions. Just like its strategies on border management and critical infrastructure protection, the RAS is designed to provide real-time updates and alerts on disinformation campaigns. The idea is that each member state will appoint a PoC and this individual should be responsible for sharing news and alerts on disinformation at the national level. This information will then be shared with networks across the Union and disinformation alerts will also be exchanged with the EU Hybrid Fusion Cell and INTCEN at the EEAS, plus with the Commission's Emergency Response Coordination Centre (ERCC). The RAS was formally established by the EU in March 2019.

TOWARDS A MORE MEDIA-LITERATE AND RESILIENT SOCIETY?

Disinformation has formed a central pillar in EU action to counter hybrid threats. While the initial impulse to act on disinformation emerged in the wake of the Ukraine crisis, the EU is also investing in countering disinformation in order to protect elections. Similarly to its strategies for border management and critical infrastructure, the EU's strategy on disinformation relies in large part on the buy-in from member states to share information in a timely fashion. This sort of 'networked' response to information exchange is logical but, as has been shown already, it is challenging to ensure that member states share quality intelligence and information. Exchange of information and intelligence is not just important for effective situational awareness, but also because one of the important aspects of countering hybrid threats is how disinformation might be part of a broader hybrid campaign against the EU. We must avoid looking at disinformation in isolation from other hybrid and/or conventional tactics. This is why it is essential that the RAS connects with other EU alert systems (e.g. CIWIN, EFS, NIS) on crisis response, border management and critical infrastructure protection. It is the fusion of data and intelligence that will make all the difference when it comes to taking political decisions on whether the EU is subject to a hybrid attack.

However, countering disinformation is made even more difficult because of the important role of private actors such as social media companies and citizens. Private actors sit on the frontline of combating disinformation and they clearly have a role in managing harmful content and disinformation. In particular, social media companies also have a responsibility for how personal data is harvested and used on their platforms. Data collection and algorithmic manipulation is on the rise and any adversary with the means to collect large-scale amounts of data can use it to better understand how, when and why societies react and engage with news but it can also give insights into the emotional impulses of societies and communities. Here, the EU's General Data Protection Regulation (GDPR) has greatly aided matters by putting in place a sanctioning mechanism (i.e. a fine of up to 4% of a firm's annual global turnover or €20 million – whichever happens to be greater) for the incorrect collection and misuse of personal data.

18 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on an Action Plan against Disinformation", *JOIN(2018) 36 final*, Brussels, December 5, 2018, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

Yet getting the regulation of social media platforms right is not easy, especially given that fundamental rights and openness must be ensured. That is not to say that social media companies are totally failing to live up to the EU Code of Practice. For example, Facebook announced in March 2019 that it had removed 2,632 pages, accounts and groups linked to Iran, Russia, Macedonia and Kosovo from Facebook and Instagram.[19] However, the European Commission made clear after the first progress reports on the Code of Practice were delivered by Google, Facebook and Twitter in January 2019 that more needs to be done. In particular, the Commission expressed its deep concern that such companies had still failed to 'provide specific benchmarks to measure progress' or to provide detailed results on the measures they had taken.[20] This concern was reiterated by the open-source web browser corporation Mozilla, which stressed that 'there is currently a lack of publicly available data about political advertising on Facebook in the European Union that can be compared to information about what ads users are seeing'.[21] Without such benchmarks and data transparency, it will be difficult for the EU to gauge the scale of the disinformation challenge in Europe and to optimise disinformation alerts through the RAS.

Facebook announced in March 2019 that it had removed 2,632 pages, accounts and groups linked to Iran, Russia, Macedonia and Kosovo.

Another challenging aspect of countering disinformation is enhancing the media literacy of the public through awareness raising, education programmes and professional courses for journalists. Here, the challenge is not just raising awareness about disinformation but rather developing skills such as media interpretation and critical engagement.[22] This is complicated by the use of new information and communication technologies such as social media. The main challenge is not just to develop the ability to decipher whether a news headline, report or message is false or not, but to also go one step further to critically assess which actors stand behind a falsehood and why they may want to promulgate it in the first place. As Figure 4 above shows, the public across many EU member states are increasingly wary of news sources but the danger is that mistrust in specific social media platforms might lead to a wider antipathy towards the press and media. EU initiatives such as the Media Literacy Week are good vehicles for raising awareness across the EU, but clearly more needs to be done at the national level to ensure that some of the core skills needed to combat disinformation are embedded in society – especially as effective StratCom should target local and regional communities, with all the cultural and linguistic nuance this implies. In order for the public to fully understand the dangers of disinformation, however, greater communication on which actors might be behind disinformation campaigns is just as important as providing training and education on the general concept of disinformation. This point is particularly crucial if we want citizens and the public to be able to connect disinformation campaigns with wider hybrid threat strategies.

19 Nathaniel Gleicher, "Removing Coordinated Inauthentic Behaviour from Iran, Russia, Macedonia and Kosovo", *Facebook*, March 26, 2019, https://newsroom.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/

20 European Commission, "First Monthly Intermediate Results of the EU Code of Practice against Disinformation", February 28, 2019, https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation.

21 "Letter to Mariya Gabriel, Commissioner for Digital Economy & Society", *Mozilla*, January 31, 2019, https://blog.mozilla.org/wp-content/uploads/2019/01/Mozilla-letter-to-EU-Commission-on-Facebook-transparency-31-01-19-1.pdf.

22 Maria Hellman and Charlotte Wagnsson, "How can European States Respond to Russian Information Warfare? An Analytical Framework", *European Security*, vol. 26, no. 2 (2017), p. 162.

CONCLUSION

This *Chaillot Paper* started off by asking how the EU can practically prevent and respond to hybrid threats. The analysis has shown that the EU has responded to hybrid threats in various ways. First, the publication of sectoral and/or overarching strategies are designed to inform and guide EU efforts. Second, the creation of new or the revision of established expert bodies focus on a particular aspect of hybrid threats. Third, developing or revising legal instruments in such a way as to better respond to hybrid threats. Fourth, investing in information-sharing mechanisms that can help better link member states with the EU level so as to enhance common risk analysis and situational awareness. Fifth, boosting the EU's preparedness for hybrid attacks through exercises and simulations. Sixth, working closely with partners such as NATO. Finally, investing in and financing the core capacities needed to combat hybrid threats.

Based on these initiatives, the EU has clearly emerged as a more credible actor in the sphere of internal and external security and responding to hybrid threats. The Union is much better placed to detect hybrid threats today than was the case before 2014. This has surely changed the strategic calculus for adversaries that are planning and launching hybrid campaigns against the Union. The EU's response to hybrid threats has helped with burden-sharing in a transatlantic context, but it also provides evidence that the EU is a more strategically autonomous actor today. This situation is unlikely to be reversed given the investments that have been or will be made in various security and defence sectors by the Commission. The proposed €13 billion European Defence Fund (2021-2027) or the €450 million invested in cybersecurity since 2016 through the public-private partnership on cybersecurity, are just two examples.

This paper has not covered every aspect of hybrid threats, nor has it sought to provide specific recommendations on how the EU can improve its counter hybrid threat strategies. Instead, the paper has focused on three policy domains – border management, critical infrastructure and disinformation – that are vital in a hybrid context. The aim was to analyse what the EU has achieved in each area, and it also endeavoured to outline the trade-offs and obstacles to further cooperation. What emerges from the analysis is that any successful strategy to counter hybrid threats will not focus simply on specific sectors but it should rather seek to pull these sectors together for an overarching strategic response. This requires joined-up institutions, close links with governments, credible and timely intelligence and, above all else, political judgment.

The truth of the matter is that hybrid threats are potent because they are difficult to detect. A threat to critical infrastructure might well be part of an overall attack on the EU that includes border tensions and disinformation campaigns (i.e. horizontal hybrid strategies). Alternatively, a coordinated disinformation campaign may be employed to set the groundwork for some later escalation (i.e. vertical hybrid strategies). In other cases an attack on critical infrastructure might not be part of a hybrid campaign at all - it could be the work of criminals, terrorists or extremists. It is for this reason that the rapid identification of and reaction to hybrid threats is challenging. It also means that high-calibre data and intelligence is required and that the Union builds up its resilience through regular exercises and learning lessons from external partners that have been subject to hybrid campaigns in the past.

Another finding in this *Chaillot Paper* is that there is still a need for better coordination among institutions, governments and the private sector. While it is perhaps a cliché to speak of silo mentalities, the reality is that there remains a partial disconnect between EU

institutions and the member states. Bodies such as the Hybrid Fusion Cell have greatly enhanced EU responses by helping to pull together the threads in multiple policy domains such as cybersecurity, disinformation, CBRN and counter-intelligence. Beyond EU efforts, however, greater efforts are needed to ensure that the private sector pulls its weight in managing critical infrastructure and disinformation in a hybrid context. While cooperation between EU institutions and agencies is a challenge in border management, a lack of information sharing pervades efforts in critical infrastructure protection. In some cases, it remains difficult to share sensitive information among EU bodies and agencies. Where disinformation is concerned, the issue is ensuring that the private sector understands the importance of hybrid threats and has an incentive to act against fake news, harmful data collection and media manipulation.

As this paper has shown, improving societal resilience against hybrid threats is clearly a mammoth task for the EU. Enhancing resilience depends upon improving media literacy, but proactive strategic communication can simultaneously refute fake news, counter disinformation campaigns and convey positive messages about the EU. Of course, the linguistic and cultural nuances of each EU member state should be factored in when devising strategic communication campaigns. Yet this does not mean that an overall positive narrative of the EU should not be created. Additionally, strategic communication and media literacy must contend with noteworthy technological shifts. Vast amounts of personal data are being harvested online, sometimes for nefarious reasons. Using Big Data to ascertain what makes societies fearful or what will damage their morale and trust in governments will become an increasingly difficult factor in combating disinformation.

Improving societal resilience against hybrid threats is clearly a mammoth task for the EU.

Additionally, this paper has pointed to instances where responses to hybrid threats may raise questions about how fundamental rights are managed. The case of border management clearly highlights the tension between the need to keep borders as open as possible and ensuring effective management of them. Disinformation raises the potential tension between open societies and a need to ensure that harmful and false information is expunged from online platforms. Even the case of critical infrastructure shows that a careful balancing act is required between maintaining an open economy and ensuring that Europe's vital supply networks and infrastructure are not exploited by competitors and adversaries.

Beyond the seemingly binary choices that may emerge during the design and implementation of counter hybrid threat strategies, lies an observation about the power of the EU's norms and values. Presumably the political, economic, social and cultural make-up of the EU is precisely what attracts adversaries to employ hybrid tactics in the first place. In this respect, the Union should hold firm to its basic values when engaging in counter hybrid activities. The EU should maintain an open economy and champion freedom of expression, although it should avoid being naive when it does so. The power of the EU to counter hybrid threats rests in the Union's ability to stay true to its core values. In a hybrid context of deniability, disinformation and impunity, adhering to core values not only makes for credible strategic communication, but it also makes broader strategic sense because it reassures partners and domestic audiences. Unity of purpose and the cohesion of various EU actors - governments and institutions alike - is ultimately the basis for any sound strategy against hybrid threats.

GLOSSARY

astroturfing

Producing and disseminating the message that there is widespread and popular support for an idea, product, politician, individual or campaign when there is not.

asymmetric threats

Tactics and strategies that are designed to exploit weaknesses and vulnerabilities in powerful military and political actors.

attribution

The process of proving that a particular actor or actors are responsible for a malicious activity.

black out

To experience a disruption in critical infrastructure such as electricity or the Internet.

botnet

A network of computers infected by malware and controlled by a master source.

clickbait

The use of sensationalised headlines and/or stories that are designed to attract media consumers' attention.

cognitive bias

An attempt to simplify information based on one's bias and experiences.

commodity continuity

The probability that a commodity will continue to be traded and available in the face of supply disruption.

compound warfare

The simultaneous use of regular and irregular warfighting capabilities under a unified command.

computer-mediated communication

A method of communication that is supported by the use of electronic devices such as mobile phones.

confirmation bias

The consumption and engagement with media sources that confirm one's own beliefs. Also known as an 'echo chamber'.

conspiracy theory

A theory that tries to advance improbable and/or false ideas in contrast to more credible explanations for social phenomena.

contingency plan

A strategy that is designed to deal with the fall-out from future events.

counterculture

A method of living, attitudes and/or norms that contradict prevailing social norms.

covert operations

Military operations designed to allow the adversary to deny responsibility.

critical infrastructure

Systems, services, nodes and networks that are considered vital for the proper functioning of society and the economy.

cultivation

The process of attracting and gaining wilful and unwitting supporters for a cause or disinformation campaign.

data war

Any war or conflict that sees the weaponisation and use of data.

data warehouse

An online storage database that houses collected data from numerous sources.

decoding

The process of uncovering and/or understanding political messages designed to spread fake news, disinformation and propaganda.

demarcation

The boundaries or borders of a geographical space or state territory.

deniability

A process of denying knowledge and responsibility for aggressive political and/or military actions.

denial of service

The malicious interruption of a computer service by blocking user access to this service.

doxing

A process of gathering and publishing private information on an individual with a view to discrediting or harming them.

disinformation

False or inaccurate information purposefully disseminated in order to wilfully deceive the public.

dummy firm

A firm or company that is established to serve as a cover for nefarious or malicious economic activities.

expected energy unserved

A metric that is designed to measure the security of supply or reliability of an energy resource.

fake news

Stories that are fabricated with the intent of instilling doubt, fear and confusion in society.

filter bubble

The use of algorithms that target and customise news sources for individuals based on age, gender, location, browsing history, etc.

Gerasimov doctrine

Theory of modern war based on the blurring of lines between conventional and unconventional means, tactics and strategies. The doctrine is named after Russia's Chief of the General Staff, Valeri Gerasimov.

heuristics

Rapid problem solving without necessarily weighing up costs and benefits rationally due to time and cognitive restraints.

hoax

A false message that is deliberately disseminated in order to cloud or confuse the truth.

horizontal escalation

The process of geographically expanding a conflict through the use of economic, diplomatic and military means.

information flows

Flows of information that can either be top-down in nature (government to society) or bottom-up in nature (society to government).

information weapon

Sensitive information that can be turned into a weapon against an adversary or competitor.

integrated border management

A process of coordination and cooperation among relevant authorities, governments, agencies and international organisations to ensure border management.

kompromat

This Russian word refers to compromising material intended for use against an adversary, usually for the purposes of blackmail or intelligence recruitment.

loss of load probability

A metric that is designed to measure whether the consumption of an energy resource will outstrip supply.

malware

Software that is designed to gain malicious access to computer systems with the intention of disrupting and damaging these systems.

media literacy

The process of informing, educating and alerting society to the dangers of fake news and disinformation.

meta narrative

An explanation for the overarching narrative, purpose or meaning of social phenomena, often used as guidance for targeted strategic communications, disinformation and/or propaganda.

misinformation

False or inaccurate information unwittingly disseminated in the public domain.

narrative strategies

A technique employed to meaningfully create and disseminate stories or narratives that support one particular political objective or interest.

open source

Freely available information or data that can be redistributed, modified and used (usually without consent).

psychological sphere of influence

Commanding political messages to such a degree that whole societies (or sections of society) are easily manipulated or their morale can be controlled.

ransomware

Software designed to maliciously block use of a computer system or network until a demand is met.

resilience

The ability to recover rapidly and effectively from a crisis or conflict.

risk assessment

A process of evaluating potential risks that may arise from political action.

sock puppet

A fake online account created by a person or group for the purposes of trolling.

subversion

A process and strategy designed to overthrow the principles and established ideas and norms of a society.

synchronisation

The combination and sophisticated use of multiple capacities in order to conduct a hybrid campaign.

system of systems

The existence of individual and separate systems that interact, are interdependent and form part of a wider meta system.

trolling

The act of posting comments, photos or other forms of online content, normally from a fake account, with the deliberate purpose of eliciting an emotional response from online users.

vertical escalation

Tactics and strategies designed to expand conflict by using unconventional means and/or capabilities in an adversary's territorial space.

web brigade

A group of sock puppets, usually supported by a state actor.

wicked problem

A social problem that is difficult or impossible to solve because of incomplete data and information about the causal factors of a problem.

zone of impunity

A geographical or virtual space in which an actor or actor can undertake political action without fear of retribution or punishment.

ABBREVIATIONS

5G
Fifth Generation Network

AFSJ
Area of Freedom, Security and Justice

BCP
Border Crossing Point

CBRN
Chemical, Biological, Radiological and Nuclear

CFSP
Common Foreign and Security Policy

CIWIN
Critical Infrastructure Warning Information Network

COE
Council of Europe

CoE
Centre of Excellence

CPM
Civil Protection Mechanism

CSDP
Common Security and Defence Policy

CSIRT
Computer Security Incident Response Team

DG Home
Directorate General for Home Affairs

DG HR
Directorate General for Human Resources and Security

DoS
Denial of Service

EASA
European Aviation Safety Agency

ECG
Electricity Coordination Group

EDA
European Defence Agency

EDF
European Defence Fund

EDIDP
European Defence Industrial Development Programme

EEAS
European External Action Service

EFS
Eurosur Fusion Service

ENISA
European Union Agency for Network and Information Security

ENTSO-E
European Network of Transmission System Operators for Electricity

ENTSOG
European Network of Transmission System Operators for Gas

EPCIP
European Programme for Critical Infrastructure Protection

ERCC
European Response Coordination Centre

ESTA
Electronic System for Travel Authorisation

ETIAS
European Travel Information and Authorisation System

EU
European Union

EUMSS
European Union Maritime Security Strategy

EUNAVFOR
EU Naval Force

EURODAC
European Asylum Dactyloscopy Database

FDI
Foreign Direct Investment

FoP
Friends of the Presidency Group

GCG
Gas Coordination Group

GDPR
General Data Protection Regulation

GPS
Global Positioning System

GSMC
Galileo Security Monitoring Centre

HAMSPRO
Harbour and Maritime Surveillance and Protection

HR/VP
High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission

HUMINT
Human Intelligence

IBM
Integrated Border Management

IBMF
Integrated Border Management Fund

IMF
International Monetary Fund

INTCEN
EU Intelligence and Situation Centre

IPCR
Integrated Political Crisis Response

KGB
Committee for State Security (*Komitet gosudarstvennoy bezopasnosti*)

LBTA
Local Border Traffic Agreement

LNG
Liquefied Natural Gas

MCDC
Multinational Capability Development Campaign

MFF
Multiannual Financial Framework

NATO
North Atlantic Treaty Organisation

NGO
Non-Governmental Organisation

NIS
Network and Information Systems

OCEAN2020
Open Cooperation for European Maritime Awareness

OCG
Oil Coordination Group

OLAF
European Anti-Fraud Office

OSCE
Organisation for Security and Cooperation in Europe

PACE
Parallel and Coordinated Exercise

PADR
Preparatory Action on Defence Research

PESCO
Permanent Structured Cooperation

PoC
Point of Contact

R&D
Research and Development

RAS
Rapid Alert System

SBC
Schengen Borders Code

SLO
Security Liaison Officer

SOCTAS
Serious and Organised Crime Threat Assessments

STAR
Strategic Analysis and Response

StratCom
Strategic Communication

TEU
Treaty on European Union

TFEU
Treaty on the Functioning of the European Union

UAV
Unmanned Aerial Vehicle

UK
United Kingdom

US
United States

WTO
World Trade Organisation

Hybrid threats – unconventional threats that fall under the threshold of military force – have become an ubiquitous feature of today's security environment.

Although the EU is much better placed to detect and combat hybrid threats today than was the case five years ago, this new form of asymmetric conflict remains a major challenge.

This *Chaillot Paper* seeks to provide practical and operational insights on how the EU can best respond to and counter hybrid threats. It focuses on three key policy domains that are of vital significance in a hybrid context – borders, critical infrastructure and disinformation – and shows how the EU has developed specific strategies to combat hybrid challenges in these areas. The paper underlines the importance of developing an overarching strategic response, and of improving coordinated EU approaches to hybrid threats.

EUISS European Union Institute for Security Studies

Publications Office

ISBN 978-92-9198-833-4
CATALOGUE NUMBER QN-AA-19-002-EN-C

© European Union Institute for Security Studies, 2019.