Safer Together
Strengthening Europe's Civilian and Military Preparedness and Readiness

Report by **Sauli Niinistö**, former President of the Republic of Finland,
In his capacity as Special Adviser to the President of the European Commission

Contents

PREFACE

— p. 4

EXECUTIVE SUMMARY

— p. 13

CHAPTER 01

Decoding the crises of today and anticipating the threats of tomorrow

— p. 31

CHAPTER 02

Enabling the EU to function under all circumstances

— p. 46

CHAPTER 03

Ensuring speed of action with structures and procedures that are fit for purpose

— p. 58

CHAPTER 04

Empowering citizens as the backbone of societal resilience and preparedness

— p. 71

CHAPTER 05

Leveraging the full potential of public-private cooperation

— p. 86

CHAPTER 06

Outsmarting malicious actors to deter hybrid attacks

— p. 103

CHAPTER 07

Scaling up Europe's defence efforts and unlocking its dual-use potential

— p. 118

CHAPTER 08

Building mutual resilience with partners through assertive EU diplomacy

— p. 138

CHAPTER 09

Harnessing the economics of preparedness by investing together upfront

— p. 156

FOREWORD

On 20 March, the President of the European Commission, together with the High Representative / Vice President, asked Special Adviser Sauli Niinistö – Former President of the Republic of Finland – to write a report on how to enhance Europe's civilian and defence preparedness and readiness by October 2024. This report has the purpose of assessing the complex challenges the EU and its Member States face in a volatile geopolitical landscape and present recommendations to enhance the preparedness and readiness of the EU[01].

The following questions guided the work on the report:

- how to improve risk identification, anticipatory analysis, strategic foresight, and early warning as a driver for coordinated action;
- how to mainstream civilian and military preparedness across sectors to overcome a silos approach and enhance EU resilience;
- how to ensure the necessary civilian and military capabilities are fit for purpose to prevent, recover from and respond to crises of different origins while ensuring that response mechanisms and structures are well coordinated (EU and national level) and;
- how to foster civil-military cooperation as well as public-private partnerships and leverage international partnerships to strengthen our preparedness;
- how to enhance the awareness and resilience of EU citizens and societies.

The analysis in the report builds on and complements various relevant work strands that are already ongoing, notably in the context of horizontal crisis management, the implementation of the Strategic Compass as well other relevant EU strategies, initiatives and policies across sectors, including the civil protection, defence industry, hybrid threats, critical infrastructure, cyber security, disinformation, space, military mobility, maritime security, health and food security, economic security, etc. It draws on consultations with stakeholders across the EU institutions and bodies, Member States, relevant international organisations, representatives of the private sector and experts from think tanks and academia.

The report is intended to inform, inter alia, future actions to be proposed by the High Representative and the Commission in the light of the Political Guidelines for the next Commission (2024-2029), as put forward by President von der Leyen, and her mission letters to the incoming Commissioners and High Representative. It is offered moreover as an independent analytical assessment that may provide inspiration to decision-makers in all EU institutions and Member State capitals.

01. Press statement 24/1602 of 20 March 2024 - Press statement by President von der Leyen with former Finnish President Niinistö.

PREFACE

Preparing Europe for a more dangerous world

Security is the foundation on which everything is built

The European Union's security environment has in many ways taken a turn for the worse in recent years. The world is more dangerous and crisis-prone. The continuation of peace cannot be taken for granted and security cannot be seen as a given, as is manifested by the increasing damage caused by climate change. We must be better prepared, not only to survive, but also to thrive in this new reality. This calls for an overhaul of the way we Europeans see the Union's role in keeping us all secure.

The objective of European integration after the Second World War was to create lasting peace among its members. It was seen that only peace and security make development and people's well-being possible. This created a new European spirit and a new idea of cooperation that has taken long steps forward. This is a great achievement of the countries and the community that form today's EU.

Despite all the wars, conflicts and disasters that have taken place in the EU's neighbourhood and beyond, the EU and its Member States have been secure from immediate existential threats since the end of the Cold War.

During the first decades after the Cold War, it became easy to think that security is not something that is a very present concern in our daily lives. Yet, in fact, we need security for everything. This applies equally to individuals, communities, States, and the whole European Union. We cannot see and feel security when we have it, which makes its loss all the more dramatic and painful.

At the start of this decade, Europe has woken up to a new reality. The COVID-19 pandemic was a crisis of a nature and magnitude for which all Member States and the EU as a whole were insufficiently prepared. Russia's full-scale invasion of Ukraine showed that it takes two to maintain peace, but only one to start a war. Russia's invasion also underlined Putin's long-held perception that the West and Western people are weak. Moreover, the increasing damage caused by extreme weather events is forcing Europeans to ask not only how climate change will affect future generations, but also what we need to prepare for today.

The structures, processes and legal basis of the EU have been created over decades without our own security needs at their core. For example, the EU's common foreign, security and defence policies, as well as cooperation on internal security, were all launched in the 1990's when direct threats to the EU were perceived to be at a historic low. What's more, the gravity of the threat of climate change for our livelihoods and way of life had not yet been fully understood.

The optimism of that time stands in sharp contrast to today's security environment. This is increasingly shaped by great power competition and the readiness of authoritarian States to use violence to assert their territorial or political claims. In addition, instrumentalised migration and, for example, disruptions to global supply chains underline the multifaceted nature of threats. We need to make sure our legislation, working methods and tools match the challenges we face. However, at its heart, preparedness is an attitude.

A new mindset to preparedness

The need for better preparedness forces us to consider our mindset and even our values, and how to defend them from a new perspective.

A prerequisite for preparedness is to understand that security is the foundation of everything we hold dear. Security is a public good – the most important thing that everyone needs. It is the precondition for maintaining our values, as well as being a necessity for our economic success and competitiveness. If we lose security, it takes with it our well-being and our plans for the future.

Our democratic political systems and rule of law are based on the protection of individuals' rights and the provision of a broad open space for people to exercise their freedoms. This open space is exploited by malicious actors, as we constantly see in the diverse hybrid operations conducted against us.

Open societies provide both an ideal model for individuals to exercise their rights and a perfect opportunity to hurt us. A key underlying question that has guided the preparation of this report is how to protect our values without undermining them in the process.

Lenin instructed the Bolsheviks during the Russian civil war to 'probe with bayonets: If you find mush you continue. If you find steel you stop'. A hundred years on, today's opportunistic actors use the same method. They target us by looking for weaknesses in our protection, take advantage of our political divisions, any lack of social cohesion and harmful economic dependencies, trying to weaponise anything they can against us. In being well prepared, a fundamental requirement is not to be an easy target.

A change in mindset is needed to build the trust that allows us to do this as the whole of society.

This change needs to take place across the full spectrum of the EU's activities. Preparedness requires a high level of trust between public authorities, Member States, EU institutions, the private sector, and civil society. Ultimately, preparedness begins and ends with the trust of citizens that the political community they live in is worth protecting and defending. Evolving threats, such as the sabotage of critical infrastructure and cyberattacks, continue to bring private and public actors' security interests ever closer. The systematic sharing of information and experiences is crucial for further deepening trust between different actors to prepare for and address these threats together.

Leaders have a responsibility to articulate clearly to citizens the threats we need to be prepared for. Raising public awareness of the risk landscape without creating panic and involving citizens more closely in building security is of paramount importance. We have several good examples of this in Europe. New options are currently being considered in many Member States – not only in the form of conscription, but also through other legal obligations citizens have to contribute to security and preparedness in different capacities. Voluntary engagement and participation in the activities of civil society organisations should also be further encouraged in this context. More active involvement can be asked when citizens trust that their leaders are prepared to keep them secure and are able to protect them throughout any crisis.

A common interest like preparedness requires common responsibility. Each individual has a stake in building and maintaining security, for example by choosing what kind of information sources we trust. Understanding everyone's responsibility for their own security and that of those closest to them makes it easier to accept the actions and investment needed from Member States and the EU to build stronger preparedness.

EU citizens are already expressing clearly their expectations for the Union to become a stronger security actor. In a Eurobarometer poll conducted across Member States in spring this year, for example, 77% of respondents confirmed their support for the EU's common security and defence policy and 71% stated that they want the EU to do more to reinforce the production of military equipment.

There is also an increasing awareness of the need for preparedness for disasters on a personal level. In a September 2024 Eurobarometer, 58% of respondents replied that they did not consider themselves well prepared for a crisis in the area where they live. Almost two-thirds feel that they need more information to prepare for disasters and emergencies.

Single security

EU Member States have a legal and moral obligation under the Lisbon Treaty (Art. 42.7) and the Treaty on the Functioning of the European Union (Art. 222) to show solidarity and support one another during crises. However, these legal commitments have not been fully transformed into an attitude where security is seen as something shared across the EU.

Security is understandably perceived very much in a regional context. For example, the threat of Russian aggression is felt most acutely by its immediate neighbours. Worsening droughts, flooding, and other manifestations of climate change are most acute concerns in those areas where they have already been experienced. In reality, the most serious threats we need to be prepared for come with wide-ranging consequences that cross borders. Their impact cannot be prevented without common action.

We must understand that a threat to the sovereignty of any Member State affects the integrity of all others in the Union as well. The territorial integrity and political independence of every Member State is inextricably linked with that of other Member States, and the EU as a whole. If one Member State loses its security, it poses a problem for the others too.

Our societies, economies, physical and digital infrastructure, and networks needed to move goods, services, money, information and people are deeply integrated. This deep integration is not only what makes our Single Market function and enables our prosperity. It also needs to be seen as a tool that enables us to prepare for and work efficiently and systematically together during crises to address shared threats with common solutions.

The EU is key to better preparedness

The EU has already proven to be indispensable in crises that are too large for any Member State to prepare for and overcome individually. The Union's role was instrumental in addressing the COVID-19 pandemic, including the rapid development and successful distribution of vaccines, and in organising Member States' support for Ukraine.

Yet, in responding to the pandemic and Russia's aggression against Ukraine, our action was initially focus on reacting to shocks with ad hoc solutions and improvisation. We need to move from reaction to proactive preparedness.

For the EU to be a fully fledged security actor, it must be prepared to maintain its own vital societal and institutional functions under all circumstances. It must be able to take decisions and implement them in the chaotic conditions of a major disaster. To provide support to the regions most in need, key functions of the EU, including the Single Market, must be kept operational no matter what to avoid competition for scarce resources between Member States, uncoordinated closures of internal borders, and other hindrances to efficient common action. This is a key demand in preparing for armed aggression and other most extreme threat scenarios.

Greater preparedness cannot be built by trying to isolate ourselves from the outside world. We must address external threats from a position of strength together with partners across the globe in ways that uphold and strengthen the rules-based international order. The EU's diplomacy must be geared to take the shared security interests we have with third countries more fully into account, and concentrate even more on addressing and eradicating where possible the root causes of external risks for our security. We must prepare for different threats by working beyond our closest like-minded partners to support the resilience of third countries and cooperate with them in ways that at the same time benefit our own preparedness.

Preparedness is a matter of credibility. Insufficient preparedness amid increasing threats weakens the trust that citizens place in public authorities. If there are doubts about our ability to function and deliver

during a major crisis, it will also diminish our value in the eyes of partners. Equally, inadequate preparedness invites malicious and opportunistic actors to target us to an even greater extent.

The fact that all Member States find themselves in the same boat sailing in choppy waters applies to our security as much as to our economy. The fundamental need to improve our competitiveness was recently highlighted in the report by Special Adviser Mario Draghi. The link between competitiveness and security works both ways, and is of particular importance taking into account that the EU's share of the world economy and its population are shrinking. Only a Europe that is competitive economically is able to keep itself secure and influence global developments, rather than merely adapting to them, and to provide the best environment for businesses to grow and succeed.

The current state of the EU's preparedness

Today, the EU is more able to deal with major crises and disasters than it was five years ago. Important pieces of legislation, mechanisms and tools across different policy areas, including health security, cybersecurity, defence and critical infrastructure resilience, have been developed or reinforced.

However, the multifaceted changes in our security environment have outpaced the speed of our action.

Despite the significant improvements in many sectors, there is an urgent need to enhance preparedness for all hazards and our readiness for major crises and disasters in a strategic way. We need to be prepared to deal with several major crises that may be connected, taking into account that crises do not occur in silos, or in orderly succession.

We need better preparedness to ensure that in the future the EU will not be taken by surprise by events we should have seen coming. Any major crisis includes unexpected elements, but the better prepared we are for anything that we can reasonably anticipate, the more capable we will be to deal with unforeseeable events.

This report proposes a step change in the way we think about and act on preparedness in the EU. For many years already, the EU has developed preparedness capabilities in individual sectors, in particular in the fields of civil protection and disaster management. Instruments, such as the Union Civil Protection Mechanism, have proven their value in practice. This is a good basis to build on, but looking at the EU as a whole in a deteriorating global security environment, two gaps are particularly evident:

- We do not have a clear plan on what the EU will do in the event of armed aggression against a Member State. The threat of war posed by Russia to European security forces us to address this as a centrepiece of our preparedness, without undermining the work to prepare for other major threats. This includes those connected to disruptions to the global economy, disasters driven by climate change, or another pandemic.

- We do not have comprehensive capacity to bring all necessary EU resources together in a coordinated manner across institutional and operational silos to prepare for – and if needed, act – in response to major cross-sectoral and cross-border shocks and crises.

Preparedness is still often misunderstood as a separate policy area, or something that would cover only certain aspects of the EU's functions. Instead, it must become a way of thinking, planning and acting that cuts across all sectors. While there must be clarity of leadership, organisation and coordination structures inside and between the EU institutions, everyone under the 'EU umbrella' should be involved and tasked with taking responsibility for preparedness within their own areas of responsibility.

Preparedness is built with actions instead of words. A realistic understanding of what we are currently capable of doing in the most challenging scenarios is necessary to understand where greater efforts must be made.

We must also be able to analyse threats and threat actors with greater accuracy. Making better use of intelligence analysis and foresight in the EU's policy planning and decision-making enables us to do so. For example, recognising earlier Russia's ability to mobilise its war economy and limit – or at least postpone – economic hardships could have underlined the urgency of our efforts to arm Ukraine, and to estimate sooner and more accurately the scale of long-term support needed during a protracted war.

Our ability to prepare for and act to tackle major threats is currently constrained by institutional, legal and political limitations that make it too difficult to bring relevant actors together quickly to address threats and manage a major crisis. One particular example is that defence and military security is still handled in the EU, to a large extent on a national basis, and in isolation from other fields of EU policy. Due to these limitations, developing new military capabilities urgently needed in Europe is slower, at a smaller scale, and more expensive than it should be.

This divide must be bridged in our structures and our mindset. Most crises are not military in nature and militaries alone do not offer all solutions. Yet, in preparing for the most significant security threats, including armed aggression with all its consequences, the link between militaries and civilian authorities and the rest of our societies must function effectively. This is also a key demand for EU-NATO cooperation in the preparedness context and an issue on which several Member States are currently working to create national models for enhanced cross-sectoral preparedness, and the ability to act in the event of war and other major crises.

Preparedness to maintain peace

We need preparedness and strength not to wage war, but to maintain peace. The risk of Russian aggression beyond Ukraine cannot be excluded. Preparing for this risk is not escalatory in any way, but rather intends to discourage Russia or any other actor from targeting the Union and its Member States. Improving the defence capabilities of EU Member States is necessary to ensure that they are able to support one another in line with their obiligations under the EU treaty and contribute to a strengthened deterrence.

The EU is one of Ukraine's most important supporters when putting together military, economic and humanitarian aid, and we have a lot to learn from its brave defence against Russia. Ukrainians are fighting against a combination of hybrid and conventional means of warfare in all domains. Ukraine has, for instance, learned to use intelligence efficiently to support decision-making, to bring new technological innovation, such as inexpensive drones, rapidly to the front; to acquire massive amounts of weaponry and ammunition, and to train and mobilise hundreds of thousands of troops. It is showing every day what defence in a long war of attrition against an aggressor like Russia demands. This war also underscores the significant gaps Member States have in their own military readiness.

Stepping up our defence readiness and industrial capacity must take into account that 23 out of 27 EU Member States are NATO allies. NATO is the foundation of its members' collective defence and the bedrock of Europe's security to military threats. However, aggression against an EU Member State belonging to NATO would also fundamentally affect the EU as a whole. This would require a response deploying all the EU's tools and resources across policy areas from agriculture to space, and the economy to diplomacy.

When the EU Member States belonging to NATO fully meet their obligations as NATO Allies, they will be able to make a stronger contribution to a 'more European NATO'. NATO's European members must be ready to fill any gaps and additional needs created by changes in the global security environment, for example if the US would commit an increasing share of its military resources to the Asia-Pacific region. Cooperation within the EU is key to enabling the creation and production of the additional capabilities this would require. While the EU and NATO are separate, they share the goal of keeping Europe secure.

In preparing for military aggression against an EU Member State and a NATO ally, we must ensure that the two organisations are ready to work hand in hand, have a clear division of tasks, and see how

collective defence under Article 5 and measures in the EU mutually complement and strengthen each other in the best way. As Ukraine's example also shows, no military defence can be successful without keeping the economy running, providing basic services and critical goods for civilians, ensuring the mobility and communication of the military and other crisis actors, while supporting the resilience of citizens and society.

A European approach to comprehensive preparedness

This report proposes a conceptual and practical approach to comprehensive preparedness for the EU. It presents the evolving threat landscape from the point of view of preparedness and makes concrete recommendations to enhance the Union's level of preparedness and readiness to act in major crises, as called for by the European Council in its Conclusions from March 2024 and with a view to President von der Leyen's 2024-2029 Political Guidelines for the next European Commission.

In the context of this report, preparedness refers to the EU's ability to:

- anticipate
- prevent
- withstand; and
- respond to major threats or crises that a) concern the EU as a whole, or more than one Member State with broad cross-border and cross-sectoral effects; and b) are of a magnitude and complexity that require resources and policies beyond national capacities.

A sufficient level of preparedness for any threat must be measured by three criteria:

- how serious the threat and its potential consequences are;
- how likely the threat is to materialise; and
- what capabilities and actions are needed to prepare for it.

Preparedness is not about an 'either/or' choice between preparing or not preparing for different types of threats. The focus of EU-level measures needs to be on the most severe scenarios. These pose many similar requirements for the Union's ability to function and contribute to the protection of citizens under exceptional and difficult circumstances, irrespective of the nature and origin of a particular threat.

Preparedness must start by analysing the full spectrum of threats against which we must be able to protect the Union and its Member States. Chapter 2 of this report deals with the current threat landscape and assesses key trends for the years ahead.

From chapter 2, the report provides short analyses and key recommendations on how to systematically strengthen the EU's preparedness, ranging from addressing immediate needs to mid and long-term processes. The EU Treaties provide the necessary legal basis for comprehensive and much more ambitious preparedness. All proposals are made in keeping with the competence of Member States as defined in the Treaties concerning their responsibilities in matters of national security, and in line with the principle of subsidiarity.

When making recommendations for future action, the starting point of this report is to build on the means we already have in the EU to support in different ways our preparedness, while also recognising the gaps where new tools and solutions are needed.

Being adequately prepared for major threats requires working according to a whole-of-government and a whole-of-society approach. These frequently repeated terms mean in practice the ability to develop and use in a concerted and coordinated fashion all the necessary tools and resources across different policy areas, while engaging the private sector, civil society organisations, and citizens.

Preparedness for today and tomorrow's threats cannot be built in silos, country by country, or separately in different sectors of government. Comprehensive preparedness requires interaction. For example, cybersecurity risks concern both public authorities and private companies in similar ways. Preparing for them must be done together as closely as possible, taking advantage of the information and legal means available to public authorities and the technical know-how and capabilities of private companies. The role of civil society organisations is also crucial, for example in raising awareness and training the skills and preparedness measures every individual needs.

Preparedness must also be seen as a key component of deterrence against malicious State actors and their proxies.

Deterrence is not how the EU has traditionally defined its role in security, but in facing a constantly evolving threat landscape, this must change. We must make it as difficult as possible for threat actors to achieve any of their intended objectives. In addition, preventing or even limiting the increasing sabotage and other hybrid operations requires that perpetrators face consequences that are much more severe than they are today. Perceptions matter, perhaps most importantly in the eyes of threat actors. They still seem to consider the EU weak, slow and disintegrated in our ability to prevent and, in particular, respond to malicious activities, from espionage on our territories to potential threats against our space capabilities, and everything in between.

Pandemic, war and other kinds of long-lasting crises affect all parts of societies and economies, can cause massive numbers of casualties, and challenge the ability of the authorities to provide basic services to citizens. Our preparedness must take into account that the consequences of these most serious threats may not be limited to a temporary disruption of the status quo, but result in profound and irreversible changes to our security environment and societies. Many threats, including hybrid operations, cyberattacks, disinformation campaigns, economic coercion and damage caused by climate change, are already taking place continuously. Preparedness is needed to signal to potential adversaries that they will not be able to outlast the EU.

While consensus among all 27 Member States or a qualified majority is the precondition for moving ahead with many of the structural, legislative and organisational changes proposed in this report, we should also be open to launch new initiatives enhancing preparedness, where needed only among willing Member States, to enable faster action.

Together from the lowest to the boldest common denominator

Maintaining peace and providing security that allows people to live in freedom and prosperity remains at the heart of the European project. What in the 20st century was created through integration to eliminate the reasons for conflict between European nations must now be achieved by becoming as prepared as possible to face any threat together with unity, strength and resolve. Preparedness cannot be built on the hope that worst-case scenarios will never materialise.

Member States have at the national level prioritised different threats based on their geography, historical experiences, resources and other factors. These differing threat perceptions should not be a hindrance to being better prepared together. We all need the same core institutional and societal functions, goods and abilities to protect our citizens, regardless of the nature and origin of a specific threat.

Looking at the magnitude of the threats we face, we cannot limit our level of preparedness to what is politically convenient, or where the lowest common denominator between Member States currently lies. This approach will not work, because it will not be enough. We must be able to take more risks together as the EU to limit the national exposure of Member States.

Many of the proposals made in this report will no doubt be difficult to reach consensus on among Member States. On the other hand, it is hard to imagine that if we would be faced with an immediate existential threat to our Union, we would not be able to cross the red lines, political sensitivities and mental blocks that under normal circumstances often keep the EU from reaching its full potential. We have already shown in the past years that when crisis hits, we are able to come together. Being prepared in advance for the next event of this kind increases the likelihood of success and diminishes related costs, or in the best case makes it possible to avoid a crisis altogether.

The EU needs to take more strategic responsibility for security in Europe, and this must be fully reflected in our preparedness. This is an important signal to the US and other key partners with whom we have a shared interest to continue and deepen our long-standing close cooperation. If we are not doing everything we can for our own security, we cannot ask anyone else to do it for us. The need for stronger European responsibility for our security will remain beyond individual elections or political cycles in the US. The more we are ready to do together as the EU, the more we can expect our partners to be willing to contribute to our shared preparedness.

Preparedness is a precondition for the EU to have the strength to defend its citizens, interests and values. Only the strong ones will be able to thrive in a dangerous world. Weak ones get pushed around and divided ones are taken advantage of.

Preparedness requires a clear-eyed understanding of this reality, yet it is the opposite of pessimism and hopelessness. Europeans should not forget that we have achieved historic success in developing a social model and a political community that continue to inspire and attract more nations to join our Union, while also offering a chance to disagree and tolerate a plurality of opinions. In today's world, this in itself is worth protecting.

Making the EU better prepared for the risks and threats we face depends on us. We have the necessary financial and other resources to become safer together. The only open question is if we have the political will to prioritise the long-term benefits of a fully prepared EU over its short-term costs. It is also a question of our readiness to change the ways we work together to ensure our ability to respond to cross-border threats with cross-border solutions.

It is high time to put preparedness at the heart of the EU's work. The world around us will not wait for Europe to be ready.

Sauli Niinistö
Special Adviser to the President of the European Commission
Former President of the Republic of Finland (2012-2024)

ACKNOWLEDGMENTS

This report is the result of dedication and engagement of a large number of exceptional people, who have embarked with me into the complex dimensions of the preparedness and resilience of Europe.

I would like to acknowledge the President of the European Commission Ursula von der Leyen, and her team, for her constant support and guidance throughout the development of the Report, and to thank the High Representative / Vice-President Josep Borrell, and his team, for his invaluable support.

This Report would not have been possible without the excellent work of the support team put together in I.D.E.A. (Inspire, Debate, Engage and Accelerate Action). Sonia Vila Núñez, Arnout Molenaar, Turo Mattila and Giacomo Köhler oversaw and coordinated all the work on the report. The analysis and the policy advice contained in the report owes much to the contributions of Marianne Ardisson, Daniele Bianchi, Max Brandt, Jonas Cederlöf, Andrei Franceschi Popescu, Benjamin Hartmann, Tomasz Husak, Mihnea Motoc, Alexander Hempfing, Julia Stewart-David, Jean-Pierre Van Aubel and Maarten Vergauwen. The editorial assistance provided by Thomas Hopkins was also greatly appreciated. The team could count on the precious support of Sven Kilemet, Carmen Tresguerres and Henna Kurvi.

Lastly, I would like to acknowledge the important contributions and relevant discussions I had with many European Commission, international organisations' and Member States' officials and experts, representatives of the private sector, trade unions and employers' organisations as well as experts from civil society organisations, think tanks and academia.

EXECUTIVE SUMMARY

Key findings

- **Facing a new reality** – Since the start of this decade, the EU has experienced the most severe pandemic in a century; the bloodiest war on European soil since the Second World War; and the hottest year in recorded history. The COVID-19 pandemic was a crisis of a nature and magnitude for which all Member States and the EU as a whole were insufficiently prepared. Russia's full-scale invasion of Ukraine showed that it takes two to maintain peace, but only one to start a war. Russia's invasion also underlined Putin's long-held perception that the West and Western people are weak. Moreover, the increasing damage caused by extreme weather events is forcing Europeans to ask not only how climate change will affect future generations, but also what we need to prepare for today. These deeply disruptive events are neither transitory nor isolated. They are driven and connected by underlying fault lines, long-term shifts and root causes that point to a prolonged period of high risk and deep uncertainty for the Union. We need to awaken to a new, unstable reality and there is no reason to expect that the underlying driving forces will dissipate in the foreseeable future.

- **Security as the foundation** –Stronger preparedness of the EU requires a new mindset. The return of war to Europe as well as the recent experience of the pandemic and the increasing damage connected to climate change have been stark reminders that security is the foundation of everything. Security is a public good – the essential precondition for maintaining our values and democratic political system, as well as our economic success and competitiveness. The territorial integrity and political independence of every Member State are inextricably linked. If the security of one Member State is breached or its sovereignty violated, this directly concerns the other 26 and the Union as a whole. We share a single security. EU Member States have a legal and moral obligation for solidarity and mutual assistance in accordance with the EU Treaties. Preparedness for the increasing threats we face requires a high level of trust – between the Member States and EU institutions, and between public authorities, the private sector and civil society. The starting point of preparedness is that EU citizens trust that the political community they live in is worth protecting and defending.

- **Preparing for worst-case scenarios** – Despite the steps taken to improve the EU's crisis preparedness in recent years with new legislation, mechanisms and tools in different policy areas, the EU and its Member States are not yet fully prepared for the most severe cross-sectoral or multidimensional crisis scenarios – especially given the further deteriorating external environment. The multifaceted changes in our security environment have outpaced the speed of our action. On the horizon, we can see not only the pervasive effects of climate change and increasingly brazen hybrid campaigns (including elevated risks of major cyberattacks and acts of sabotage), but also the increased threat of armed aggression against an EU Member State directly. Moreover, any future shock, disruption or crisis will take place in the context of a globally connected European economy and society that faces a fragmenting global order, more intensive strategic competition and rivalry, and an accelerating pace of disruptive technological innovation. This in turn creates an imperative to better join up different sectors so as to be able to swiftly mount a comprehensive, coherent, and decisive response when a crisis erupts. It is not only about a sense of urgency, but also a sense of agency. Raising our preparedness and readiness to a new level will shape, adapt and lower the driving factors that have led to these crises and disasters in the first place. It will help to deter aggressors and contribute to lowering the scale and impact of climate change.

- **Shifting to comprehensive preparedness** – The EU needs to adopt a robust all-hazards, whole-of-government and whole-of-society approach to its civilian and military preparedness and readiness. The report is structured around the overarching objective of building 'comprehensive preparedness' to ensure that the EU and its Member States can continue to function under all circumstances. This requires a collective capacity to effectively anticipate, prevent, withstand or respond to any type of

major shock or crisis with cross-sectoral and cross-border implications and the potential to threaten the Union as a whole. To this end, this report identifies the necessary overarching building blocks – set out below – to frame and operationalise comprehensive preparedness, in line with the Treaties and fully respecting the key roles and responsibilities of the EU and its Member States.

- **Putting citizens at the core of preparedness** – Preparedness can only be successful with the active participation of citizens. Raising public awareness of the risk landscape without fostering anxiety and empowering citizens to be able to take more responsibility for their individual preparedness is of paramount importance. Participation of citizens in different roles and capacities to supporting preparedness on societal level through voluntary and mandatory means is crucial also for social cohesion in crises. Similarly, private companies have a crucial role as producers and suppliers of critical goods, as operators of critical infrastructure and services, and developers of new innovations, solutions and capabilities needed to tackle different threats.

- **Safer together** – Despite the distinct nature and origin of different shocks, emergencies, and crises, they also have many things in common and underline the need for a stronger role of the EU as a political, economic and security actor. Threats don't stop at our borders, they cascade between the interconnected sectors of our economy, they undermine the well-being and safety of our citizens. This requires enhanced cooperation in the EU framework when the scale of the threat or crisis is beyond the capacity of individual Member States.

- **Identifying the boldest common denominator** – Member States prioritise different threats and hazards based on their geography, historical experience, resources, and other factors. These differing threat perceptions should not be a hindrance to better preparing together. All Member States need similar core institutional and societal functions, goods and capabilities to protect our citizens, regardless of the nature and origin of a specific threat. Looking at the magnitude of the threats we face, we cannot limit our level of preparedness to what is politically convenient or corresponds to the lowest common denominator between Member States.

- **Taking more strategic responsibility**– Stepping up the EU's civilian and military preparedness and readiness needs to enable the Union to take more strategic responsibility for security in Europe. This is an important signal to the US and other key partners. If we are not doing everything we can for our own security, we cannot expect others to do it for us. This includes that the Member States should strengthen their cooperation on European defence, jointly investing more to close long-standing gaps in our military and defence industrial readiness. This is also necessary to be able to support Ukraine in the long-term in a way that creates the conditions for a lasting peace on Ukraine's terms.

- **Speed is of the essence** – When major cross-border crises erupt, rapid decision-making and action are vital to mitigate the impact and to limit potential cascading effects. Over the years, the EU has developed a large number of sectoral crisis management mechanisms. Enabling the necessary speed during multidimensional crises, however, requires greater clarity of organisation, more effective decision-making and a coherent set of tried-and-tested coordination mechanisms. Moreover, it will rely on full access to the necessary data and information that enable effective decision-making. To meet the demands of the most severe threats, we need to strengthen our ability to cooperate across silos, to reinforce cooperation between different operational authorities, and streamline unnecessarily complex structures.

- **Reinforcing civilian-military cooperation** – A key dimension of comprehensive preparedness is to ensure that civilian and military crisis response actors enable each other and can operate seamlessly, including to prepare for the most severe military contingencies. For such scenarios, the EU and its Member States will need the capacity to effectively mobilise a whole-of-government response, both in support of military efforts and to protect our citizens, and shield our economy. The military also contributes to civilian-led disaster response. The EU's potential for enhanced civil-

military cooperation and dual-use infrastructures and technologies should be further unlocked, while respecting the different nature, needs and priorities of civilian and military actors. This involves optimising the use of scarce resources and strengthening coordination mechanisms for the most severe crisis situations.

- **Enhancing EU-NATO cooperation** – A strong EU-NATO partnership is essential in this context. The two organisations already address common challenges drawing on their respective toolboxes in line with their respective mandates. While recognising the different tasks and mandates of each organisation, as well as their autonomy of decision-making and respective competences, this report identifies the need to map out within the EU what the implications of major military contingencies would be, in coherence and complementarity with NATO. Moreover, the EU and NATO should consider ways to reinforce effective coordination and to exchange of information between staff when it matters the most.

- **Working with our partners** – Partner countries in our neighbourhood and globally often share and even stand at the forefront of the threats and challenges we face in Europe. Notably, this refers to Ukraine fighting Russian aggression and defending Europe's security more broadly, and numerous countries across the Sahel region, the Pacific Ocean and other regions at the front line of the global struggle against climate change. The EU should emphasise mutual resilience as a key element of its diplomacy and external action, with a view to elevating the Union as a trusted and reliable partner in a world marked by growing strategic competition.

- **The economics of preparedness** – The COVID-19 pandemic, together with the fallout of Russia's aggression against Ukraine, had an enormous economic impact on Europe. A higher preparedness baseline across all spheres of the EU's activities enables the economy and society to bounce back faster when a new pandemic, a major disruption, disaster or crisis hits the EU, including by protecting those most vulnerable. The drastic deterioration of Europe's security situation will need to be reflected in the allocation of budgetary resources, against the backdrop of decades of relative underinvestment in areas such as defence. Preparedness for shocks, disruptions and crises of a Union-wide scale and impact require a higher level of long-term investment in the EU framework. The lessons learned from the COVID-19 pandemic and the Russian invasion of Ukraine have shown, moreover, that we need to closely coordinate the procurement of crisis-relevant goods, making sure that all Member States have access to limited industrial capacity without driving up prices too much. Preparedness investment can boost European competitiveness at the same time, in line with the report of Special Adviser Mario Draghi.

- **Embracing preparedness by design** – The new comprehensive preparedness framework finally needs to be reflected in a 'preparedness-by-design' principle to be applied across the board when designing new legislation, reviewing regulatory frameworks or setting up new funding instruments. This new preparedness-by-design principle should also be reflected in the way we organise our economies. The 'just-in-time' principle that has been at the heart of supply chain management to maximise cost-effectiveness in an increasingly globalised economy is now being balanced with the need for greater shock absorption.

The building blocks of a fully prepared Union

Each building block is accompanied in this report by a set of concrete recommendations. They are offered as a basis for further work by the incoming European Commission, the High Representative, the Council of the EU, the European Parliament and Member States, acting within their respective competences. They tie in with the guidance and new initiatives set out in the Political Guidelines of President von der Leyen for the next mandate (2024-2029) and the Mission Letters to the incoming Members of the College of Commissioners and the High Representative.

1. DECODE THE CRISES OF TODAY AND ANTICIPATE THE THREATS OF TOMORROW

Comprehensive preparedness requires us to be clear-eyed in objectively assessing our own vulnerabilities and shortcomings. We need to be willing to anticipate and think through worst-case scenarios. The EU should continue to forge a shared view of the deeper shifts in the geopolitical, ecological, economic, societal, and technological domains – how they will increasingly affect our stability, prosperity and security in the years ahead. The different risk multipliers – intensifying strategic competition, the destabilising effects of climate change, and disruptive new technologies – are increasingly intertwined and cumulative in nature. Without ranking or prioritising risks or threats, or trying to cover them exhaustively in this report, the confluence of different risks leads to an increased probability of major cross-sectoral crises, shocks and disruptions occurring simultaneously in the years ahead:

- The rules-based global order is fragmenting, narrowing the basis for effective multilateral cooperation to address transnational challenges through global institutions.
- Extreme weather events will become more frequent and intense, in Europe and around the world, destabilising in particular communities in fragile contexts.
- Since Russia's brutal invasion of Ukraine, the security threat posed by Russia is at its highest since the end of the Cold War, even more so when considering the multi-front implications of growing tensions in East Asia and the Middle East.
- Our open and connected societies and economies are increasingly subject to brazen hybrid campaigns including cyberattacks, Foreign Information Manipulation and Interference (FIMI), sabotage and the instrumentalisation of migration.
- Strategic competition over raw materials, disruptive technologies and global influence is intensifying, linking economic and security interests more closely together.
- An arc covering major areas marked by fragility, instability, conflict and war stretches from our south to our east, with spill-over effects on the European Union that blur the lines between internal and external security.
- It remains critical to strengthen work on all strands of action in the comprehensive approach to migration and ensure effective control of the Union's external borders through all available means, including with the support of the European Union, in line with EU and international law.
- Another pandemic remains a distinct possibility to be prepared for, given the possibility of transmutations of animal viruses, as well as accelerating biotechnological innovation facilitating the development of synthetic pathogens.

2. ENABLE THE EU TO FUNCTION UNDER ALL CIRCUMSTANCES

The EU as a whole must be able to function under all circumstances to take and implement decisions and actions that protect and ensure citizens' well-being in times of crisis. The EU currently lacks an agreed, comprehensive list of vital societal and governmental functions defined at EU level. These functions not only ensure the smooth running of our societies and economies, but are also critical enablers that allow civilian and military crisis responders to operate effectively in crisis situations. Their continuity must be ensured against the full range of threats and hazards, from extreme weather events to State-sponsored interference and, in the most extreme instance, armed aggression against one or more of our Member States.

→ Develop a comprehensive EU Risk Assessment.

- To better manage risk, prepare for crises, and enhance the safety and security of our citizens, the EU needs a thorough and comprehensive all-hazards and all-threats risk assessment, covering all sectors of the EU's activities.

→ Use the upcoming Preparedness Union Strategy to put the EU on track for comprehensive preparedness.

- The strategy should define at EU level vital societal and governmental functions for which continuity needs to be ensured, including the necessary measures to safeguard the EU's own decision-making and implementation capacity.

- For each of the identified vital functions, EU-level Preparedness Baseline Requirements should be developed to guide future preparedness work. In relevant sectors, alignment with NATO's resilience baselines should be promoted, while noting that the EU's baseline requirements are defined against a more comprehensive mandate and a broader set of risks than in NATO, involving a wider set of sectors and stakeholders.

- Embed a 'Preparedness by Design' principle horizontally and consistently across EU institutions, bodies, and agencies and develop a mandatory 'Security and Preparedness Check' for future impact assessments and 'stress tests' of existing legislation. Rather than treating security or climate considerations as competing or mutually exclusive priorities, this principle should address both man-made and natural threats holistically.

- Coherence between and the alignment of sectoral crisis plans and blueprints at the EU level should be ensured, further clarifying 'who does what' especially in cross-sectoral scenarios.

- Set up and regularly conduct an EU Comprehensive Preparedness Exercise to test high-level decision-making, operational coordination and to build strong links between actors and across sectors. Where appropriate, this should also include the private sector, civil society, and international partners.

→ Explore the feasibility of an EU Preparedness Law to set joint standards and long-term targets, aligning EU and national efforts wherever possible.

- The law could set uniform preparedness standards and measurable targets, with the European Parliament and the Council agreeing together on principles, standards, and targets that will guide crucial EU preparedness efforts. It should streamline decision-making, coordination, and information sharing processes, and further clarify roles and responsibilities at the EU, national, and local levels.

→ Articulate a coherent vision for the EU's role in preparing for and responding to external armed aggression.

- To make sure the EU is ready to act in support of a Member State in the event of an attack, we need to assess the possible societal, economic, security and other implications and identify needs for additional measures, in complementarity with NATO. In this type of scenario, the EU will need to be able to mobilise its full spectrum of policies and tools, and related regulatory and financial powers.

→ Strengthen the EU-NATO interface in view of grave crisis situations, including through an emergency protocol that can be activated to streamline information exchange.

- In full respect of the agreed EU principles that govern the EU-NATO partnership, further joined-up work with NATO should be encouraged to identify civil-military and EU-NATO intersections and potential bottlenecks in major crisis situations.

- Both organisations could agree on an emergency protocol that could be activated in or ahead of a crisis situation, defining terms for enhanced information exchange and dialogue when it matters the most.

3. ENSURE SPEED OF ACTION WITH STRUCTURES AND PROCEDURES THAT ARE FIT FOR PURPOSE.

Rapid decision-making and action can already be a challenge in a national setting. At the EU level, there are additional interinstitutional complexities, including regarding the availability of data, large number of actors and the challenge of cross-sectoral coordination. While respecting all relevant competences, the EU should strengthen the EU's capacity for timely and well-informed decision-making – both at the political and the technical-operational level – as well as for agile follow-through and implementation. This requires organisational clarity and the further streamlining of procedures wherever possible. To this end, the EU and its Member States need to further develop an effective and efficient division of roles and responsibilities, a coherent and resilient coordination set-up, and reflexive information sharing for major crisis situations.

→ Reinforce cross-sectoral operational coordination:

- Develop a central operational crisis 'hub' within the Commission to facilitate cross-sectoral coordination and situational awareness. The hub should firmly build on the existing Emergency Response Coordination Centre (ERCC), acting as a platform to connect to relevant sectoral arrangements. The ERCC should continue to serve routine civil protection, disaster relief, and humanitarian coordination functions, but could be redesigned as a body that provides a single cross-sectoral entry point for major cross-border and cascading crises to ensure the optimal use of resources and infrastructure.

- Further optimise the use of the Integrated Political Crisis Response (IPCR) arrangements to enhance EU-level coordination and reinforce links between political leadership and the technical level.

- Strengthen civil-military coordination frameworks and joint planning to ensure an effective civil-military response to a range of intentional threats – both within and beyond the EU. This could include potentially moving towards a European Civil Defence Mechanism, as envisaged in the Political Guidelines, reflecting relevant developments in Member States. The ERCC and its further evolution into a central crisis hub should further strengthen its links with the civilian and military crisis management structures in the EEAS.

- Further operationalise Articles 42.7 TEU and 222 TFEU to strengthen their credibility and operational value as expressions of a European spirit of mutual assistance and solidarity. To this end, the EU and Member States should better define potential cases for the use of the Solidarity Clause (e.g. hybrid attacks or pandemics), adjust the activation thresholds of the Solidarity Clause to cover earlier stages of a crisis, and consider coordination needs in the event of parallel activation.

→ Boost and better coordinate situational awareness, anticipation, and foresight:

- Link situational analysis and intelligence assessments more closely with EU-level preparedness and decision-making processes. In particular, this would require strengthening the pooling of information gathered by different sectoral situational awareness capabilities.

- Set up an EU Earth-Observation governmental service for enhanced situational awareness in support of preparedness, decision-making and the action of the EU and Member States in the fields of security and defence. This would complement and build on existing capabilities provided through the EU Satellite Centre.

- Develop tools and frameworks to make EU strategic foresight more actionable and solution oriented. Building on existing work strands of the Commission's Joint Research Centre (JRC), foresight products should be made more actionable and the connection between our foresight toolbox and preparedness work should be strengthened.

→ Strengthen information sharing and communication.

- Accelerate the roll-out of secure, autonomous, and interoperable information exchange and communication systems (both terrestrial and space-based) to connect EU institutions, bodies and agencies, Member States authorities, and key partners, ensuring the rapid, continuous, and trust-based exchange of critical information.

- The EU should complete the European Critical Communication System (EUCCS) as soon as possible to securely connect all EU civil security and public safety authorities across borders. To enhance civil-military cooperation and facilitate a genuinely 'whole-of-government' response, the EU and Member States should also allow for its interoperability with systems used in the defence domain.

- Enhance the trust-based sharing of sensitive information between willing Member States for specific purposes, for example in the cyber domain.

- Embed communication more closely in horizontal and vertical crisis management, including through the development of EU frameworks and modules, as well as training for local, regional, and national contact points.

→ Enhance the EU's exercise and training culture.

- The EU should further develop a comprehensive exercise culture to make sure coordination and information sharing frameworks and relevant instruments, work in practice – even in the most disruptive crisis conditions. To this end, the EU could adopt an EU-wide Exercise Policy to promote shared approaches across different sectors and institutions, and bring together resources and expertise in a centrally accessible Exercise Knowledge Hub.

- Set up regular cross-sectoral EU training courses on security, defence, and crisis management to further reinforce mutual trust and promote a common European security, safety and preparedness culture.

4. EMPOWER CITIZENS AS THE BACKBONE OF SOCIETAL RESILIENCE AND PREPAREDNESS.

The EU and Member States can best protect citizens by enhancing their resilience and agency. This means enabling citizens – in different capacities – to play an active role in ensuring crisis preparedness and first response. They are an integral part of a 'whole of society' approach that brings together not only public authorities at all levels, but also private entities, employers and trade unions, civil society organisations, and individual citizens. Actively engaging citizens in crisis preparedness starts with raising their risk and threat awareness. This needs to be accompanied by attention to citizens' psychological resilience, mental well-being, and long-term capacity to cope with an environment characterised by heightened risk and volatility. Building on this, citizens' ability to act in the face of disaster or adversity needs to be bolstered by reinforcing individual and household preparedness and readiness across the board.

→ Enhance individual and household preparedness:

- Jointly invest in citizens' risk education, incorporating different dimensions, such as cybersecurity, disaster risks, and disinformation. The gradual integration of crisis preparedness and risk

awareness, as well as media and digital literacy, into education programmes and curricula across the EU could be an additional option to ensure structural investment in societal resilience

- Promote a target of 72-hour self-sufficiency through coordinated information campaigns. Building upon ongoing work in the context of 'PreparEU', the EU should aim to ensure households throughout the EU are prepared for minimum 72-hour basic self-sufficiency in different types of emergencies and taking into account national differences, (e.g. by providing guidelines on stockpiling, evacuations, CBRN situations, access to medical services or schooling in emergencies, etc.).

- Involve civil society organisations, trade unions and employers to enhance preparedness in different walks of life. These actors should be encouraged to use their networks to help people to receive verified and trusted information on preparedness, and to learn necessary skills to improve their own level of preparedness in different contexts, including in workplaces.

→ Improve crisis and emergency communication to reach citizens under all conditions.

- Member States' crisis communication or alert apps and other back-up early warning systems should be regularly tested and surveyed for gaps and for interoperability. Lessons learned on the use of these systems during the COVID-19 pandemic in Member States and during other major recent disasters, notably sudden onset extreme weather events, should be analysed to guide further efforts.

→ Prepare to better tackle vulnerability to crises and disasters:

- Further invest in disaster risk management for people disproportionately affected by disasters and other crisis situations, ensuring inclusive disaster preparedness at the community level. The EU and public authorities at all levels need to pay extra attention to reducing the vulnerability to disasters of certain groups, such as the elderly, people with disabilities, people with chronic diseases, and pregnant women.

- Prepare in advance to minimise the disruption of protracted crises on social cohesion and the socio-economic fabric of our societies. Concrete proposals to bolster the crisis preparedness of vulnerable groups and regions at risk of being left behind could be further developed as part of the upcoming EU Anti-Poverty Strategy announced in the new Political Guidelines (2024-2029).

→ Address the skills gap and risk of labour shortages during crises and promote active citizenship:

- Implement forward-looking measures, such as mapping workforce needs, training new labour force segments, facilitating skilled worker inflow, or putting in place labour mobility mechanisms. With its Internal Market Emergency and Resilience Act (IMERA), the EU already has a concrete tool to facilitate the free movement of workers and service providers in crisis situations. Further steps may be needed to address skills gaps and the risk of shortages in sectors critical to crisis preparedness.

- Develop targeted incentives to increase the appeal of careers in defence, security and emergency response among younger generations, working together with trade unions and employers' organisations. Possible actions could be introduced as part of the Quality Jobs Roadmap announced in the Political Guidelines (2024-2029). Structured exchanges among Member States could help to identify best practices in relation to national service and conscription models, education programmes, the build-up of functioning reserve systems, etc. that can serve as inspiration to others, are potentially transferable, and can be further facilitated at the EU level.

- Reinforce channels and opportunities enabling the active participation of young people in preparedness action by stepping up support for the voluntary sector. The EU should explore

additional opportunities to volunteer for crisis preparedness through existing EU programmes, such as the European Solidarity Corps, and step up dedicated engagement with established youth movements on crisis preparedness – for instance, in the context of the upcoming Youth Advisory Board announced in the Political Guidelines (2024-2029).

5. LEVERAGE THE FULL POTENTIAL OF PUBLIC-PRIVATE PARTNERSHIPS.

Past crises have clearly demonstrated that the private sector's preparedness and resilience is vital to ensuring critical functions for societies and the EU as a whole. Private and public businesses (for example, State-owned companies) provide essential goods and services, such as energy, transport, food, water supply and wastewater disposal, and medical supplies that are critical in times of crisis. Interdependencies between different sectors and across borders create the potential for severe knock-on effects in crisis situations, as we have seen in recent years. The recent succession of crises and disruptions have exposed different vulnerabilities in the EU's supply chains. This has led to delays, price fluctuations, disruptions, shortages and other problems for consumers that affect the EU's ability to prepare for and withstand the next crisis. Moreover, the private sector has become increasingly aware of security and geopolitical risks that might affect their businesses.

→ Enhance public-private cooperation to facilitate resilience-building, as well as swift and coordinated responses to future crises:

- Develop stronger public-private information sharing and coordination mechanisms to strengthen mutual and reciprocal exchanges on existing and emerging risks. This is crucial to enable businesses, Member States' competent authorities and the relevant EU institutions, bodies and agencies to be alerted and take the necessary precautions.

- Consider targeted and temporary flexibility measures and emergency provisions in legislation to better enable the private sector as a preparedness and crisis response actor. The EU could comprehensively screen existing legislative and institutional frameworks to identify bottlenecks and specific issues. The EU could also build on pandemic-era ad hoc derogations from State aid rules to develop a more structured and anticipatory approach to derogations in times of crisis.

- Extend and formalise public-private crisis cooperation arrangements with the Commission that successfully enabled the acceleration of the development and authorisation of treatments and vaccines, as well as the management of the energy crisis.

- Systematically integrate private sector expertise in the development of preparedness policies and emergency planning. This would enable policy-makers to better tailor policies to the needs and capabilities of critical private sector actors, and enable them to cooperate more effectively with public authorities in crisis response.

- Integrate the 'preparedness-by-design' principle in the revision of the public procurement Directive. The review should make the public procurement process not only simpler and faster, but fit for purpose in light of new challenges and risks linked to preparedness, economic security, critical infrastructure resilience, and defence, while respecting the EU's international obligations.

→ Reinforce private sector crisis preparedness and resilience:

- Raise business' awareness of the need for better preparedness and ensure a consistent level of crisis preparedness through joint public-private training and simulation exercises.

- Extend the critical infrastructure resilience framework established under the CER and NIS2 directives to other crisis-relevant sectors, including notably Europe's defence industrial base. To complement the implementation of these Directives, which provide a basis for protecting critical

infrastructure against a wide range of threats, it could be explored to broaden their scope to other critical sectors and industries vital to the maintenance of core governmental, societal, and economic functions.

- Establish a targeted physical resilience framework for key manufacturing to enhance crisis preparedness and shock resistance. The production of highly specialised goods, such as semiconductors, aircraft and spacecraft, communications and security equipment, and specialised machines and vehicles needs to be ensured in times of crisis. The EU and its Member States should extend on a targeted (company level) basis existing resilience-enhancing frameworks to manufacturing, in doing so supporting key players that help to ensure the EU's vital functions.

- Engage with businesses in institutionalising de-risking efforts, cross-sector stress tests and proactive security measures. This could build on successful examples, such as the energy sector stress tests. Critical projects for the Union, e.g. submarine cable and pipeline infrastructure, need to be meticulously screened to avoid new vulnerabilities,

- Establish industry-specific preparedness frameworks and sector-agnostic standards to mainstream resilience, preparedness and readiness planning in the private sector. This could be systematically promoted when new EU legislation is proposed, or existing legislation is revised.

→ Develop a comprehensive EU Stockpiling Strategy to incentivise coordinated public and private reserves of critical inputs, and ensure their availability under all circumstances.

- While fully acknowledging Member States' role in the domain of stockpiling and strategic reserves, joint action at the EU level could help to strengthen the EU's strategic autonomy and contribute to the de-risking of excessive external dependencies in terms of raw materials and other crisis-relevant goods.

- Map ongoing efforts, best practices and needs; jointly identify a comprehensive set of essential inputs (e.g. foodstuffs, energy, critical raw materials, emergency response equipment, medical countermeasures); and define targets to ensure minimum levels of preparedness in different crisis scenarios, including in the event of an armed aggression or the large-scale disruption of global supply chains.

- Ensure coherence and coordination between future initiatives and ongoing or proposed EU-level stockpiling efforts, for instance in the field of health preparedness, disaster and emergency response, energy, critical raw materials, and defence readiness.

- Strengthen the EU's ability to monitor in real time critical supply chains, production capacities and public and private stocks of select items and resources to ensure a sufficiently agile approach to stockpiling, including through an enhanced public-private partnership based on trust and mutual information sharing.

- Develop a set of operational criteria to guide the coordinated release of emergency reserves and stocks during emergencies or supply disruptions, and explore options to replenish strategic reserves through joint procurement or innovative financing options.

6. OUTSMART MALICIOUS ACTORS TO DETER HYBRID ATTACKS.

The significant increase in the number of malicious activities on the EU's territory points to an increasingly brazen and aggressive nature of hybrid activities by Russia and other external threat actors. The EU has already taken steps to build preparedness and resilience against hybrid threats, including most recently with the adoption of a sanctions framework for destabilising activities against the EU and its Member States. Yet, more work needs to be done to credibly deter malicious actors. Enhanced EU preparedness against hybrid threats needs to create a higher threshold for malicious actors to engage in hostile activities targeting us by strengthening our deterrence: a) through 'deterrence by denial', increasing the EU's resilience by tackling vulnerabilities and strengthening its capacity for damage mitigation; b) through 'deterrence by punishment', dissuading potential perpetrators through a decisive response that imposes costs outweighing any potential benefits of continued hybrid operations. While keeping fully in line with our democratic principles and values and respecting EU, national and international law, strengthening our preparedness is crucial in anticipation of the possible further escalation of hybrid campaigns.

→ Strengthen EU intelligence structures step-by-step towards a fully fledged EU service for intelligence cooperation.

- Implement the steps agreed by the Council as part of the implementation of the Strategic Compass to reinforce and improve Single Intelligence Assessment Capacity (SIAC), including the Hybrid Fusion Cell.
- Ensure a structured and coordinated process to timely address information requirements and requests for SIAC products, including from relevant Commission services and the EU agencies under their oversight.
- Strengthen and formalise information and data sharing arrangements between SIAC and other relevant EU level actors with a view to better aggregating information.
- Enhance cooperation between SIAC and relevant security departments/units of the Commission, the EEAS, the General Secretariat of the Council and other EU institutions and Member States to coordinate specific counter-espionage tasks.
- Develop a proposal together with Member States on the modalities of a fully-fledged intelligence cooperation service at the EU level that can serve both the strategic and operational needs of policy planning decision-making without emulating the tasks of Member States' national intelligence organisations, including in respect of their role in intelligence gathering.

→ Reinforce the EU's capacity for 'deterrence by denial':

- Take joint action to make it as difficult as possible for hostile intelligence services to operate in the EU. Discrepancies in Member States' counter-intelligence practices, legislation and insufficient cross-border information sharing can be exploited by malicious actors.
- Encourage Member States to proactively share information about vulnerabilities that pose a broader threat within the Union and should be tackled together at the EU level.
- Establish an anti-sabotage network to support Member States in preventing and responding to sabotage incidents. The network would build upon existing EU-level cooperation, notably the Critical Entities Resilience Group, the Protective Security Advisory Programme, the work of the INTCEN Hybrid Fusion Cell, and the cooperation between Member States' intelligence/security services, law enforcement, border and coast guards (including Frontex), customs and other competent authorities.

- Strengthen the links between the work on countering hybrid threats and economic security. Supply chain dependencies, future digital infrastructure, foreign direct investment, research security, and new clean technologies are leveraged by competing and malicious global powers to create the potential for weaponisation as part of coercive strategies.

- Ensure effective support to Member States facing instrumentalised migration at the Union's external borders.

→ Reinforce the EU's capacity for 'deterrence by punishment':

- Conduct a comprehensive assessment of key hybrid threat actors' strategic and operational specificities to identify aims, methods, key vulnerabilities and exposures to EU countermeasures. This will help to identify, organise and grade all tools at our disposal in an actor-specific way, with the aim of altering the cost-benefit analysis of the targeted actors over time.

- Reinforce political attribution as the basis for response to hybrid threats and consider on a case-by-case basis the public use of (declassified) intelligence assessments. In line with a 'naming and shaming' logic, rapid attribution or the public use of intelligence can be an effective way to seize the initiative and place hybrid actors on the backfoot, preventing or disrupting their malicious plans.

- Ensure the creation of a robust framework for lawful access to encrypted data to support the fight of Member States' authorities against espionage, sabotage and terrorism, as well as organised crime. There are signs that in several recent cases of sabotage, perpetrators were recruited and instructed via digital communication applications. Therefore, the ability of lawfully accessing encrypted data is important to counter such threats, while fully respecting fundamental rights and without undermining cybersecurity.

7. SCALE UP EUROPE'S DEFENCE EFFORTS AND UNLOCK ITS DUAL-USE POTENTIAL.

Stronger European defence – based on a competitive and resilient European defence technological and industrial base, and strengthened defence capabilities and readiness – is of crucial importance for the EU's comprehensive preparedness. Currently, the collective inventory of the capabilities of Member States (who are often also NATO allies) continues to show serious gaps and shortfalls. This leads to critical questions of how Europe can shore up its defences – at a much faster pace and in a joined-up way – to urgently prepare for the full spectrum of military and civilian-military contingencies. This requires both delivering high-tech capabilities, which plays into our comparative technological advantage and building up sufficient mass in case any military confrontation turns to longer term attrition. Moreover, Europe's defensive capacity hinges on a whole-of-government approach, as Member States' armed forces can benefit from enhanced civil-military cooperation and dual-use technologies and infrastructures organised through the EU framework. Increasing the available funding for defence cooperation is vital to overcome endemic fragmentation and decades of underinvestment.

→ Develop an EU defence capability package for the next decade:

- Use the forthcoming White Paper on the future of European Defence to frame an ambitious long-term ambition and policy, with a view to concrete steps forward:

  - identify and map the urgent defence needs of Member States;

  - revise the existing EU politico-military Headline Goal to reflect large-scale, multi-domain and protracted external aggression;

  - develop concrete options to enhance EU-level funding;
  - promote mutual reinforcement with NATO activities and standards;
  - strengthen where possible the governance of European defence.

- Fully implement the European Defence Industrial Strategy and the related Programme. This will bolster the aggregation of demand and create new possibilities to incentivise joint development and procurement and, for example, ensure the security of supply in crisis situations.

- Identify and develop, as a matter of urgency, a set of major Defence Projects of Common Interest, underpinned by the necessary ad hoc, long-term budgetary provisions. Air defence and cyber defence have already been highlighted in the Political Guidelines (2024-2029) as concrete examples. The selected flagships should be future-facing capabilities that can make a strategic difference – both within the EU and NATO and together with Ukraine – and offer industrial benefits within Europe.

- Make available the necessary EU-level funding to incentivise and strengthen joint capability investment to prepare Europe for major military contingencies. The EU's defence-related programmes are generally designed to support and facilitate joint and collaborative projects by Member States and/or the defence industry, acting as a 'flywheel' for the rationalisation of Europe's defence sector. The overall volume of EU funds compared to national budgets is insufficient to really impact the market.

→ Strengthen Europe's capacity to provide mid-to-long-term military assistance to Ukraine.

- The EU should maintain and further strengthen its capacity to deliver military support to Ukraine for as long as it takes. This is critical to keep Ukraine in a position to defend itself against the Russian invasion. This leads to the urgent need to further ramp up defence production capacity. The EU must also be ready to fill any possible gaps in the event of a diminished level of support for Ukraine from the US.

- The European Peace Facility, as a flexible, swift off-budget instrument operating under CFSP, should be endowed with sufficient resources.

- With Ukraine on its path to EU accession, the EU should better accompany this process and structure the progressive integration of Ukraine into the European defence ecosystem, as envisaged under EDIS and EDIP. Increasingly, this means that EU defence planning needs to systematically be based on the needs of the EU-27 and Ukraine.

→ Develop the proposed Single Market for Defence products and services with tangible measures to enhance cross-border cooperation and defence industrial competitiveness.

- Rationalising the defence equipment market in the EU will benefit our competitiveness, our security and preparedness. Currently, there are various ingrained practices, regulatory hurdles and political divergences hampering a more integrated Single Market for defence products and services.

- Lowering the barriers to cross-border cooperation on both the demand and supply side would be key to reducing the structural cost inflation of defence products, which has a detrimental impact on the purchasing power of national governments.

→ Strengthen dual-use and civil-military cooperation at the EU level, based on a whole-of-government approach:

- Conduct a review of the EU's dual use potential across all relevant domains to identify new synergies, for example through further work on priority (dual-use) transport corridors for military movements, the extension of fuel supply chains for the armed forces along these corridors; stockpiling and strategic reserves of energy, minerals and other critical goods, hospitals and medical services, maritime surveillance and monitoring systems, governmental space-based navigation, communication and observation services, etc.

- Further examine and harmonise dual-use definitions in various relevant EU funding instruments and policies. Within each area, the legal and regulatory margins should be fully explored, taking into account the specificities of the sector and defence-related actors respectively.

- Strengthen dual-use research and defence innovation in the EU framework to avoid Europe from lagging further behind the leading powers to the detriment of its long-term strategic position. Enhancing synergies between defence and civil security applications would optimise the use of scarce resources. We can build further on proposals in the report by Special Adviser Mario Draghi on the future of European competitiveness.

- Defence and dual-use-related considerations should be fully embedded in the EU's work on critical (foundational) technologies, such as AI and quantum, especially in terms of promoting the EU's advances in this field to reduce dependencies and protect against technology leakage.

- Strengthen links between the defence industry and other strategic industrial sectors that form part of the same ecosystem, such as naval/shipbuilding, space, aerospace, etc. The defence sector forms part of a broader strategic industrial ecosystem that relies on similar or interchangeable raw materials, technologies, skills, machines, and other industrial infrastructure.

- Develop a structured civilian security capability development programme to better coordinate investments in the distinct but parallel areas of civil security and defence. Such a process should be supported by consistent EU funding schemes. This would, however, require structurally reforming planning in the highly fragmented civil security sector, moving towards greater agility, standardisation and collaboration.

8. BUILD MUTUAL RESILIENCE WITH PARTNERS THROUGH ASSERTIVE EU DIPLOMACY.

Many of the threats, risks and challenges set out in this report either originate abroad, have a strong cross-border dimension, or are global and overarching in nature. The EU should therefore use its diplomacy and partnerships in a concerted fashion to strengthen mutual resilience with its partners – based on shared interests and in line with our principles and values. The EU needs to navigate its international partnerships in the context of all-pervasive strategic competition and contestation. To engage new and emerging partners in a long-term effort to build mutual resilience, the EU should further invest in its convening power and diplomatic outreach at all levels; become more strategic in its engagement with partners, and set clear priorities to avoid the risk of being stretched too thin; focus its offer on where it can offer the greatest added value, rather than competing where we cannot do so effectively; and become more agile, while delivering faster. By helping to strengthen our partners' resilience, we are also consolidating our own. The widening and deepening belt of instability and fragility needs to be treated as a key issue of concern for the EU's preparedness.

→ Embed the mutual resilience principle in upcoming EU policy initiatives – taking into account sectoral or regional specificities.

- This should be based on horizontal parameters to extrapolate the EU's interests and priorities and identify partners' resilience needs through an iterative outreach process.
- While acknowledging the very different settings of individual sectoral policies, applying these key parameters would allow mutual resilience to be integrated by design into new sectoral and cross-cutting strategies, plans and initiatives.

→ Use scenario-based risk assessments to prepare EU crisis response options and guide wider policy development on possible external shocks and crises:

- In a volatile world, our preparedness is served by more pro-actively anticipating possible external crisis scenarios. This work can feed into prudent planning for concrete crisis response options, as well as into wider EU policy development.

→ Strengthen outreach and diplomacy to involve and engage with partners at all levels:

- The EU should reach out more proactively and systematically at all levels to communicate a clear commitment to developing mutual resilience partnerships, and to rebuild long-term trust.
- Promote mutual resilience by working through multilateral fora and supporting the UN's agenda for the future. EU diplomacy should remain geared towards strengthening the capacity of relevant international institutions, in particular the UN system, to support and coordinate global efforts on mutual resilience.
- Expand the availability of EU-level early warning and threat detection tools and instruments to partners as part of partnership agreements.
- Strengthen the structural exchange of expertise, best practices and training on mutual resilience. Different sectoral dialogues, platforms or networks should be further strengthened, rolled out and equipped to deliver concrete projects. To facilitate cross-sectoral and comprehensive exchanges, the EU should consider setting up a network of regional 'Mutual Resilience Centres' with partners.

→ Conduct horizontal stock-taking and mapping of the overlapping mutual resilience interests and collaborative opportunities with partner countries as part of the planning for the next Multiannual Financial Framework:

- In the course of 2025, ahead of the next MFF, the EEAS and Commission services, together with Member States, should take stock of ongoing actions and envisioned needs in the context of mutual resilience, in different policy and geographical clusters. This gap analysis should pave the way for a greater strategic focus and enable a number of practical, regulatory and funding improvements.

→ Plan better, deliver faster:

- Review and reform processes, tools and instruments to ensure faster delivery. Speed is increasingly a determining factor for the EU's impact and leverage in a fast-paced and crisis-prone world.
- As part of an upgraded Team Europe approach, promote joint strategic planning between the EU and Member States in relation to mutual resilience and the external dimension of preparedness. This would help to maximise the impact of Team Europe initiatives and strengthen our message coherence, overall partnership offer, and leverage vis-à-vis partners.

- Embed resilience-building and preparedness into the strategic planning for the EU's flagship Global Gateway strategy. Across all five key thematic areas of the Global Gateway (digital, climate and energy, education and research, health and transport), the EU should ensure that relevant projects and initiatives contribute to building resilience and crisis preparedness.

→ Strengthen the EU's responsiveness to rapidly evolving crisis situations, including in fragile settings.

- As part of its own preparedness and ability to support partners, the EU needs to be ready to respond to unfolding external crises, using its full-spectrum toolbox, including the Common Security and Defence Policy.

- Further reinforce the role of EU CSDP missions and operations and coordinated maritime presence to enhance mutual resilience, including to safeguard international shipping routes and critical infrastructure. Innovative approaches could also be developed to facilitate the use of CSDP instruments in complementarity with internal security tools in the immediate vicinity of the EU's territory and territorial waters.

- Develop an integrated EU approach to address the arc of instability and fragility in the EU's wider neighbourhood and tackle knock-on effects on European security and stability. The EU should develop dedicated financing instruments and a framework for pragmatic engagement in complex political environments, working closely with Member States, International Financial Institutions, Multilateral Development Banks, and regional organisations. The aim should be to strike a balance between the need to stay engaged pragmatically, supporting local populations and avoiding providing support to unlawful or abusive ruling authorities.

- Ensure that international climate finance mechanisms are designed to reach the countries and communities most vulnerable to climate change; and reinforce EU assistance to help address the growing consequences of conflict and disasters.

9. HARNESS THE ECONOMICS OF PREPAREDNESS BY INVESTING TOGETHER UPFRONT.

Investing together in our own security and safety is one of the primary responsibilities the Union faces in an era of high risk and deep uncertainty. Preparedness for the high-risk context of the coming years and decades requires scaling up our joint investment across the board to a new level. Smart and sufficient upfront investment in our preparedness is essential to minimise the impact of crises. Robustly investing in preparedness at the EU level means ensuring that our efforts are effective, coherent, cost-efficient, and mutually reinforcing. There is an opportunity to connect the EU's competitiveness and preparedness investment. The daunting scale of the overall investment needs means that Europe should harness the economic and strategic potential of these investments primarily to the benefit of the Union's economy and citizens – including their comprehensive preparedness. While preparing for the next multi-year EU budget cycle starting in 2028, it also needs to be taken into account that our preparedness has urgent needs that should be addressed already before that.

→ Mainstream preparedness across the next EU budget:

- With a view to the preparation of and negotiations of the next MFF and taking into account the increasing risks in the EU's security environment, preparedness should be integrated by design in the EU budget.

- Ensure more built-in flexibility in the next MFF to allow for a faster and scalable response to unforeseen needs that arise in the wake of emergencies and crises.

- Reinforce the long-term 'preparedness impact' of EU investment and crisis recovery spending. All major structural and regional investment supported by the EU budget – in particular the EU's Cohesion Funds – should have security risk and disaster-proofing, climate-resilience and crisis-preparedness components further mainstreamed by design.

- Adapt the EU's budgetary framework to better support multi-year funding and investment and secure the long-term financing of key preparedness investment. The EU and Member States need to make sure to offer our public and private partners the necessary investment horizon and secure a long-term commitment to preparedness initiatives.

- Ring-fence funding for preparedness action. To ensure that answering the needs of an immediate crisis does not hamper our long-term efforts, response and recovery costs must not be detrimental to further prevention and preparedness action.

- Strengthen the dual-use potential of our spending, fully exploiting regulatory margins to make sure we maximise funding benefits and added value for our civilian and military readiness.

→ Develop a European Preparedness and Readiness Investment Framework to support the EU's transition to a fully prepared Union:

- As part of this investment framework to be envisioned in the next budgetary cycle, the EU should bring together relevant instruments in a coherent package with funding levels commensurate to the scale and complexity of the evolving challenges we face.

- In line with the notion of mainstreaming preparedness, all relevant instruments across sectors should earmark a certain amount for preparedness action in their respective fields – so that, for example, at least 20% of the overall EU budget contributes to the EU's security and crisis preparedness.

- The EU and Member States should consider setting up two dedicated facilities: a Defending Europe Facility (DEF) and a Securing Europe Facility (SEF), combining relevant funding streams and avoiding fragmented, siloed instruments.

  - The Defending Europe Facility should encompass relevant defence industrial and other defence-related or dual-use instruments.

  - The Securing Europe Facility should combine all instruments and programmes linked to civil security (e.g. law enforcement and border management), civil protection, and other emergency response services, and related critical infrastructures.

  The creation of two large-scale facilities with relevant windows for different activities should facilitate the pooling of resources, enabling the EU to better leverage its funds at scale for common and overarching priorities, simplifying public and private partners' access to EU-funded programmes, and contributing to the EU's competitiveness by boosting market consolidation.

- As part of this comprehensive European Preparedness and Readiness Investment Framework, the EU and Member States should also explore further innovative ways to mobilise the necessary funding for preparedness:

  - Establish an Investment Guarantee Programme, e.g. on the model of InvestEU, to trigger private sector investment in Europe's defence technological and industrial base, or disaster and crisis-resilient infrastructure through public seed money.

  - Work with the European Investment Bank to expand funding possibilities for the defence sector beyond dual-use.

- Leverage private capital for preparedness action by providing investment opportunities for EU citizens and institutional investors.

- Leverage the synergies between the EU's work on competitiveness and preparedness. For instance, the future EU Competitiveness Fund announced in the Political Guidelines (2024-2029) could provide incentives for EU companies and economic operators to address vulnerabilities in their infrastructure or supply chains.

The building blocks of a fully prepared Union

CHAPTER · CHAPTER · CHAPTER

01

Decoding the crises of today and anticipating the threats of tomorrow

The EU is experiencing a **prolonged period of major disasters and shocks to our security, ecosystems, economy, health, and supply chains**. Stronger preparedness must build on the already existing broad foundations and be guided by analyses of the **Union's performance during the most challenging crises of the past years**.

We must learn here from our preparedness gaps at the onset of both the COVID-19 pandemic and Russia's unprovoked full-scale attack on Ukraine, respectively. The warning signs were there in both cases, but there was also a degree of **collective cognitive dissonance**; a reluctance to genuinely contemplate **that something so 'unimaginable' could become reality – even though history offers ample examples**.

True preparedness requires us to be **clear-eyed and avoid wishful thinking**, and to be able to look at our own vulnerabilities and shortcomings objectively. We need to be willing to reflect on and think through worst-case scenarios, as a basis for our work on preparedness. This is not only about a sense of urgency, but also a sense of agency. **Raising our preparedness and readiness to a new level will also shape, adapt and lower the driving factors that have led to these crises and disasters in the first place**. It will help to deter aggressors and contribute to lowering the scale and impact of climate change, for example.

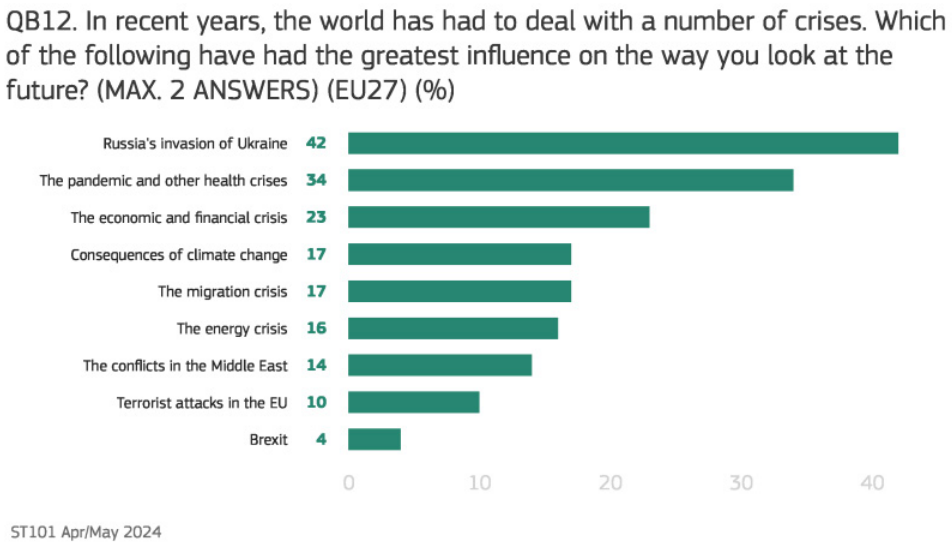
Done in the right way, effectively and sustainably, preparing for the full range of possible risks can unlock a strong **preventive and mitigating effect**. This includes avoiding that vulnerable groups and marginalised regions are disproportionately affected, as during the cost of living crisis that followed the pandemic and the soaring of energy prices triggered by Russia's invasion of Ukraine. This, in turn, has taken a toll on our societal cohesion and contributed to an increasingly polarised political culture across Europe, including an erosion of trust in government in parts of society fuelled by disinformation peddled by foreign actors[01].

01. See: European Commission, Strategic crisis management in the EU: Improving EU crisis prevention, preparedness, response and resilience, 2022.

Against this complex and dynamic background, we should continue to forge a shared view of **the deeper shifts in the geopolitical, ecological, economic, societal, and technological domains** – how they interlink and how they will together have a pervasive impact on our stability, prosperity and security in the years ahead. The following does **not intend to rank or prioritise risks – nor to be fully exhaustive**. EU Member States have **different geographical, historical and political contexts and backgrounds that influence their threat perceptions**. Threat awareness and perceptions have already been greatly converging, especially as a result of Russia's aggression against Ukraine and the recent experience of the pandemic [see Figure 1 below]. Moreover, it **is complementary to the range of risk and threat assessments** conducted at the EU level across different policy fields in recent years. This includes analyses conducted in the context of the Strategic Compass for security and defence, the Disaster Resilience Goals, and the EU's Climate Risk Assessment.

FIGURE 1

Standard Eurobarometer 101 Spring 2024

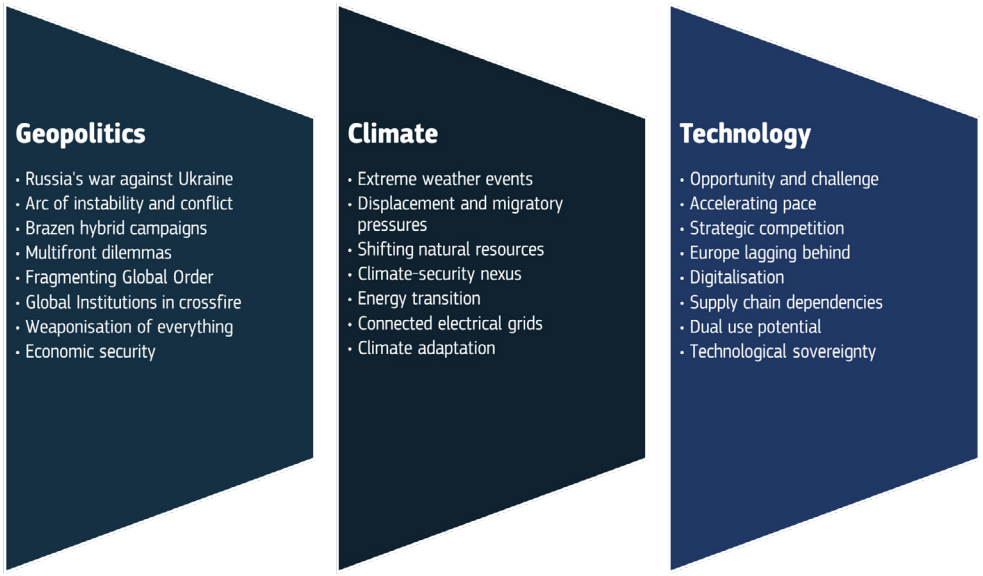


Source: Standard Eurobarometer 101, 2024.

Increased risk, deep uncertainty

The recent crises that the EU has faced are not just transitory phenomena. They reflect deeper fault lines that severely undermine the fundamentals of the international rules-based order, as well as our planet's biosphere. There is a growing expert consensus that the intensity and scale of risks stemming from ongoing **geopolitical, climatic/ecological and technological shifts will increase**. Moreover, the different risk multipliers – intensifying strategic competition, the destabilising effects of climate change, and disruptive new technologies – are increasingly **intertwined and cumulative in nature**. They have distinct impacts on Europe's overall risk profile, but also **interact with and reinforce each other**.

FIGURE 2
Macro-level shifts transforming the EU's risk environment



In combination, they are leading to an **increased probability of major cross-sectoral crises, shocks and disruptions occurring simultaneously** in the years ahead. Europeans need to be prepared for a **prolonged period of increased risk and deep uncertainty, requiring a pro-active strengthening of preparedness and resilience across all sectors**.

→ Another pandemic remains a distinct possibility to be prepared for

Pandemics have taken place throughout human history, and the risk of the next pandemic remains among the primary health threat categories identified by the Health Emergency Preparedness and Response Authority (HERA) of the Commission. As we have experienced, a pandemic can have a profound shock effect on European citizens, our society and economy, and possibly also our security and defence[02]. Its impact was magnified due to the **globalised and highly interconnected nature of our societies and economies** – which is a common feature in relation to all the various crisis risks and challenges we face.

Further transmutations of animal viruses to become infectious for humans remains a distinct possibility. Moreover, advancing biotechnological possibilities to develop synthetic pathogens, aided by AI-driven software systems, is creating new risks related to future health preparedness and weaponisation by State or non-State actors[03]. Finally, the profound changes to ecosystems as a result of global warming can increase the risks of new pandemics caused by zoonotic diseases.

→ The twin climate-environmental crisis will bring more disruptions to our daily lives.

The EU's first-ever European Climate Risk Assessment report, published in March 2024, warns of the **progressive impact of climate-related hazards** (e.g. heatwaves, prolonged droughts and floods) in interaction with non-climatic risk drivers[04] to threaten Europe's ecosystems, food security, public health, infrastructure and economy. It warned that Europe is warming at twice the rate of the global average, while being insufficiently prepared. This requires the embedding of climate adaptation and mitigation throughout all policies.

02. European Commission, Health Union: HERA delivers list of top-3 health threats to prepare against – press release, 2022.

03. Brent, R., McKelvey, T.G. Jr., and Matheny, J., The New Bioweapons. How Synthetic Biology Could Destabilise the World, Foreign Affairs, 2024.

04. European Environment Agency, European Climate Risk Assessment Report, Report No 1/2024, 2024.

In line with the climate-health and climate-social nexus, cascading climate and environmental hazards act as a **risk multiplier and can lead to system-wide challenges affecting whole societies and exacerbating existing social, economic, health and environmental risks and crises**. Certain sectors of society are particularly vulnerable to climate impacts. As those least responsible are often most affected – both in Europe and at the global level – climate change can also fuel social **contestation and unrest**.

With 2023 as the warmest year on global record, the world's ocean temperature reaching new heights, and Europe being the world's fastest-warming continent, **mitigating climate change and the degradation of nature, while adapting to their broader consequences, are key components of the EU's preparedness directly linked to our security**. The immediate reaction to geopolitical crises, for example in the context of the energy crisis in 2022, carries the risk of **delaying or deviating from the primary focus of reducing emissions and reducing our carbon footprint** as the best way to reduce climate risks in the first place.

The impact of climate change will vary in different parts of Europe, as weather patterns change and become more extreme – including **the possibility of megadroughts** that span large regions and can continue for years, but also **extreme precipitation** that increases the risk of devastating floods[05]. Beyond natural disasters, climate change will gradually affect soils and freshwater reserves, and decrease agricultural and industrial output. The structural scarcity of natural resources is a key component in defining the future global geostrategic balance of power.

→ The fragmenting global order demands a more assertive Europe.

The window for multilateral cooperation on climate change and other transnational challenges is meanwhile narrowing. **The global order is fragmenting and increasingly characterised by a complex and multi-layered multipolarity and entrenched instabilities**[06]. In particular, the economic and military rise of China in the Indo-Pacific, Russia's military aggression in Europe, and the strategic convergence between these two autocratic powers, is reshaping international relations across Eurasia and around the world – even if the majority of countries **refuse to entertain a bloc logic and are engaged in multi-partnerships**[07].

Autocratic revisionist powers defend their repressive practices at home and their regional power ambitions abroad through an **alternative vision of their respective regional security orders and the overall rules-based global order**. Tapping into legitimate discussions about global multilateral governance, they undermine basic principles of international law through their actions, while reinterpreting standards and shaping grey areas based on their underlying norms, values and interests. Consensus-based global **multilateral institutions are increasingly caught in the crossfire** of growing systemic rivalry.

This ongoing shift from cooperation to competition, even confrontation, in the global order is accelerated by a greater focus on self-reliance and a desire to reduce the economic inter-dependencies that nevertheless remain a reality after the globalisation boom of the post-Cold War years. This unstable mix of growing contestation and deep interdependence will define the global landscape for years to come, affecting both Europe's security and its prosperity.

05. European Environment Agency, Ibid, 2024.
A pessimistic scenario without additional policy action suggests that economic damage related to coastal floods alone might exceed EUR 1 trillion per year by the end of the century in the EU. Moreover, the record-hot summer of 2022 has been linked to between 60,000 and 70,000 premature deaths in Europe. A recent study estimates that the number of premature heat-deaths could rise to 95,000 every summer by 2040 and up to 120,000 by 2050.

06. It is increasingly commonplace to interpret the current global transition away from the post-Cold War unipolar US-led global order as a shift towards 'multipolarity'. However, it would be more nuanced to speak of unbalanced, layered multipolarity. The poles are far from equal; the world is complex and multi-layered. The US still dominates militarily even if China is catching up; geopolitical competition is bi-polar (with the US and China as the main poles); economic power is tri-polar (when considering the GDP of the US, China and the EU); whereas regional powers (India, Russia and to a lesser extent Iran and Turkey) and niche powers (such as Saudi-Arabia) have gained relative influence.

07. For example, Russia and China are increasingly striving to leverage the expanding BRICS group as a platform to promote anti-Western policies and positions, as well as challenge the current international order.

Combined with the twin digital and energy transition, this is fuelling a **great power competition** for resources, technology and influence. **This includes a focus on monetary alternatives that contribute to de-dollarisation, which would help to shield against the impact of international sanctions.** In the coming decade, this may also extend to growing competition over food, land, water and habitable spaces, which appears to be taken into account by actors such as China and Russia – and may become a key factor in the long-term development of their deepening partnership.

The EU therefore finds itself in a world that is characterised by the 'weaponisation of everything'08 and, with this, the securitisation of everything. The increasingly confrontational policies and actions of Russia and China towards the West have already seriously undermined the long-held conviction that trade and economic interdependencies would overcome security dilemmas; and that the economy and security could be seen as essentially separate domains.

Closer ties **between China, Russia, Iran and North Korea, in different configurations**, is leading to increasing links in terms of military cooperation, trade, finance, transport networks, proliferation, and sanctions evasion, while they are increasingly coordinating their approaches to regional crises. One recent example of this is the reported presence of North Korean troops in Russia and possible participation in President Putin's war of aggression against Ukraine. **Democratic backsliding** in many parts of the world, including Europe, is often amplified by pro-Chinese/Russian propaganda that fuels anti-democratic and anti-Western attitudes. **This creates the risk of a vicious circle of autocratic powers using propaganda and disinformation to undermine the West and gaining influence for themselves**.

The **global commons**[09] and strategic domains, such as cyber space, are increasingly contested and weaponised as part of the rising geopolitical tensions. In all these domains, there is either an ongoing contestation that undermines effective global governance or an absence of rules and norms, which increase the risks of misperception and escalation. In these areas, a growing number of State and non-State actors are striving to increase their presence.

This has direct implications for the EU. **The freedom of navigation and ensuring the security of key maritime supply routes** to Europe are key elements of preparedness, as well as an economic necessity, as 90% of the value of international trade and close to 80% of the EU's external trade is transported on the seas[10]. Similarly, the **safety and security of space systems and digital services against growing contestation and threats** is another key element, as our digital economies and societies rely heavily on space-based services [see Box 1 below].

BOX 1

Preparing for crises in space

The economy, society and governments depend on satellites to a significant degree. They not only provide navigation and communication services, but also enable digitals systems, for instance through their precision timing comparable to the atomic clock.

Space is increasingly congested. The risk of collisions is developing at rapidly and can have a catastrophic and cascading effect:

- More than 1 million pieces of debris larger than 1 cm are currently orbiting the Earth, in addition to an increasing number of satellites, with more than 50, 000 additional satellites expected to be launched over the next decade.

08. Galeotti, M., The Weaponization of Everything: A Field Guide to the New Way of War, Yale University Press, 2023.

09. International law identifies four global commons, namely the High Seas, the Atmosphere, Antarctica and Outer Space.

10. World Economic Forum, These are the world's most vital waterways for global trade, 2024.
Eurostat, International trade in goods by mode of transport, 2024.

This requires **space situational awareness** capabilities to **detect and characterise risks and hazards** in space, as well as **capabilities to protect space assets and services**. Today, the Space Situational Awareness (SSA) component of the EU space programme aims to establish a holistic approach towards the main space hazards. The **EU Space Surveillance and Tracking (SST) partnership is providing collision avoidance services to nearly 500 satellites**, as well as fragmentation and risk of re-entry analysis. Yet, the ability to autonomously detect and track space objects of interest is limited due to gaps in the sensors network and to the low sensitivity of available sensors.

Space is also an increasingly contested domain:

- With its destructive anti-satellite missile test in 2021, Russia demonstrated its capability to destroy satellites in space. This threatening behaviour entails a high risk of miscalculation and escalation, and undermines stability in outer space.
- China is increasingly aiming towards space superiority as a way of dominating the space-enabled information sphere, developing a wide range of counter-space capabilities.

The ability to detect threats in space should be enhanced at the EU level, including through capability development for space situational awareness, synergies with EU SST, and enhanced information sharing.

The EU must be able to respond to threats in space as a global actor. The EU Space Threat Response Architecture (STRA) is the framework for managing space threats/attacks to the EU, including its Space Programme. It should further evolve to allow the EU to answer to threats in space technically, politically, diplomatically or economically.

In the event of a crisis in space severely impacting the delivery of EU space-based services, the EU would face important capability gaps. Effective space capabilities would enable the quick replacement of a destroyed satellite, while civilian in-space operation and services capacity would be key to react to the loss of control of a dysfunctional space asset, to assess and repair damage, or to adapt its mission/functions. It is crucial to strengthen R&D efforts in these domains at the EU level.

More generally, the **EU needs to be prepared for potential crises in space** that are likely to arise in a near future. As commercial actors are playing a growing role in providing space-based services, including to governmental users, the effective **protection and resilience of space systems and of the space industry becomes ever-more important**. The EU should leverage its regulatory power to set up common rules for the resilience, safety and sustainability of space activities in the EU.

Strategic stability around the world is further affected by China's rapid expansion of its **nuclear arsenal,** as well as the accelerating pace of North Korea's nuclear and ballistic build-up. This is creating new deterrence dilemmas, which are compounded by the emergence of new technological advances in delivery and detection systems. Moreover, Iran remains on the brink of achieving weapons-grade enriched uranium, which could set off a wave of nuclear proliferation in the region. In line with the notion of 'aggressive sanctuarisation', nuclear deterrence is increasingly seen as a useful **cover for aggressive behaviour** by autocratic States. President Putin's aggressive nuclear rhetoric in the context of his war of aggression against Ukraine as well as Russia's stationing of tactical nuclear weapons in Belarus, suspension of its participation in the new START Treaty (the last US-Russian arms control agreement) and deliberate threats to the physical integrity of Ukraine's nuclear facilities including in Zaporizhzhia are a case in point.

→ Russia's war against Ukraine has caused a lasting change in Europe's security order.

At the epicentre of this ongoing fragmentation of the rules-based global order is **Russia's unprovoked war of conquest against Ukraine**. Russia's revisionist and imperialistic ambitions, illegally annexing territory from its neighbours and positioning itself into a long-lasting ideological confrontation with the West, mean that **the war cannot be resolved in a way that would turn the clock back to a status quo ante bellum**. This has brought about **fundamental changes to Europe's security order.**

The post-Cold War cooperative security model aspired by the EU and NATO has broken down due to Russia's aggressive and antagonistic behaviour. The latter is driven by anachronistic 'spheres-of-influence' thinking, rather than accepting its neighbouring countries' rights to self-determination. The need for **sustained and massive support for Ukraine** will remain, even in the event of a suspension of hostilities. This will be vital to ensuring that Ukraine is able to continue to defend itself against any resumption of Russian aggression at a later stage, as well as to support the Ukrainian economy and population in the huge reconstruction effort needed.

This is the best guarantee for Europe's own long-term security. The EU's full-scale support to Ukraine for as long as it takes should not only be seen as a way to keep Ukraine alive, but also of gaining a strong enough position in the long term, so that Russia no longer sees it possible to achieve its objectives. This could create the conditions for the kind of just peace Ukraine's leadership is seeking. A collapse of Western support to Ukraine would open the possibility for Russia to subjugate Ukraine and to deny its statehood and nationhood. It would be a strategic mistake for the EU to assume that even this would pacify Russia.

→ The EU and NATO need to prepare for an elevated military threat in a multifront setting.

Ukraine's ability to defend itself successfully depends on the capacity of Western countries to maintain and increase their support through the provision of military capabilities, training, economic, humanitarian and other forms of assistance. The EU's ability to support Ukraine depends also directly on our capacity to scale up the production of defence materiel to meet the increased demands of stronger deterrence for ourselves.

In the meantime, **Russia has already significantly expanded its military-industrial production capacity and augmented its armed forces**, including to offset its staggering battlefield losses[11], without setting its economy and society on a full war footing. Even though fear of increasing social tensions and financial constraints may hold it back, this also means that Russia has room for further mobilisation of manpower and additional financial resources to continuing the war into the future, while making concerted efforts to reconstitute its military capabilities beyond their levels prior to the invasion of Ukraine in 2022[12].

While most of Russia's military resources continue to be tied up in Ukraine, the rhetoric of a 'permanent war' against the 'collective West', the militarisation of Russian society and plans for expanded military presence along Russia's north-western border and in the Arctic, all point to a **further elevated risk of possible Russian aggression towards the EU and NATO**. Even though Russia's advances in Eastern and Southern Ukraine have been slow and extremely costly, there is no reason to underestimate the commitment of Russia's leadership to prioritise military spending in the long term over other priorities. In fact, **Russian defence expenditures planned for 2024 are not much lower than NATO's European member combined spending**, when weighted according to purchasing power parity, according to the International Institute for Strategic Studies [see figure 3]. According to data provided for this

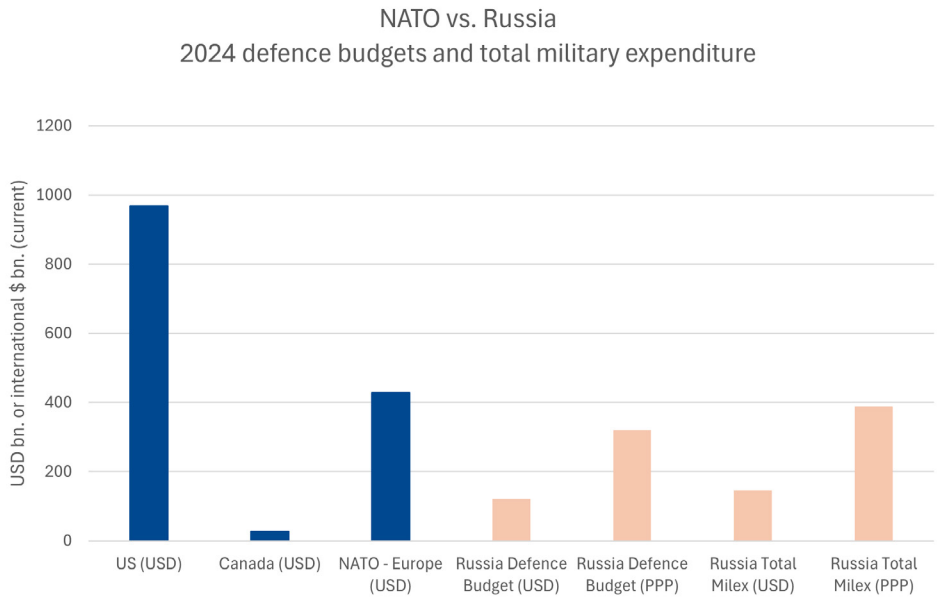
11. For example, according to public estimates, Russia is already able to produce up to three million rounds of 155 mm artillery ammunition annually, whereas the combined output of the EU and the US this year is considerably lower. In addition, Russian armed forces and society have been able to withstand extremely high losses of troops on the battlefield without creating domestic pressure for Putin to find a way out of the war or an inability to recruit new troops.

12. Massicott, D., and Connolly, R., Russian Military Reconstitution: 2030 Pathways and Prospects, Carnegie Endowment for International Peace, 2024.

report by the Institute for International Security Studies, in 2024, NATO's European members spent around USD 428 billion on defence while the estimate for total Russian military expenditure (i.e. in line with the NATO definition for defence) comes to 388 billion USD when using purchasing power parity conversions[13]. Russia has recently announced a further increase in of 25% to its defence budget for 2025, and is estimated to use almost 41% of its State expenditure and 8% of its GDP on military and security combined.

FIGURE 3

US, NATO Europe and Russian defence budgets for 2024, including purchasing power parity conversions.



Source: Based on data from IISS, 2024.

Russia remains confident that it is able to outlast Ukraine and its Western supporters with its ability to mobilise resources and the capacity to sustain human and economic losses. **Moreover, the pace of its industrial ramp-up in key domains (tanks, drones, missiles, ammunition) is higher than in Europe**[14].

China meanwhile continues to provide essential assistance to Russia, enabling it to continue its war against Ukraine. In addition, Russia is also benefitting from Iranian and North Korean military assistance. China is undergoing a comprehensive process of long-term military modernisation with the

13. International comparisons of defence spending are often based on an exchange rate conversion (Ruble-Dollar in this case). This gives a very skewed picture, however, as it does not reflect the purchasing power of the Ruble within its own economy, where the costs of personnel, materials, etc. are relatively lower. The same applies to China. The Chairman of the US Joint Chiefs of Staff, General Milley, raised this issue in Congress in 2021.
See: Robertson, P.E., 'The Military Rise of China: The Real Defence Budget Over Two Decades', Defence and Peace Economics, 2024. See also: Fravel, M.T., Gilboy, G.J., and Heginbotham, E., Estimating China's Defense Spending: How to Get it Wrong (and Right), The Scholar, Summer 2024, 40-54.

14. Reuters, Russia ramps up output of some military hardware by more than tenfold – state company, 2023
See: Center for Strategic and International Studies, Back in Stock? The State of Russia's Defense Industry after Two Years of the War, 2024.

aim of transforming the People's Liberation Army into 'world-class armed forces' by 2049[15]. China's rise and the rapid increase in its comprehensive national power are **profoundly altering the strategic balance in the Indo-Pacific**. Beyond its long-held ambitions to take over Taiwan, which it considers indispensable for the realisation of China's rejuvenation and the historic mission of the Communist Party of China (CPC), China's coercive foreign and security policies toward neighbours including India, the Philippines, and Vietnam are undermining regional stability. This creates a **risk of escalation, with the potential for simultaneous crises that would have not only local or regional impacts, but global ones**, as these developments are intertwined with the broader China-US strategic rivalry.

The **stronger prioritisation of the Indo-Pacific region in the security and defence policy of the United States** reflects a bipartisan consensus in Washington. According to the US' National Security Strategy, China is viewed as the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military and technological means to advance that objective. This shift is further amplified by political voices in the US that call for an end to US 'generosity' towards Europe, as they fear an overstretch and want to prioritise what they perceive as growing domestic problems within the US itself.

A scenario in which the US must commit more forces to East Asia due to rising tensions with China may trigger opportunistic behaviour from Russia vis-à-vis NATO directly. Experts warn that a deeply hostile and fully rearmed Russia could be tempted to challenge and test NATO's security and deterrence posture. This could even take the form of a military incursion into the territory of a NATO Ally and an EU Member State. Taking a multi-front perspective linking the Euro-Atlantic and Indo-Pacific, **strategic analysts warn of a window of high risk towards the end of the decade**[16].

The potential **economic and security impact of Chinese aggression against Taiwan or in the South China Sea would be staggering for Europe** and the world – even in grey-zone scenarios in which China stops short of war, but escalates drawing on coercive measures, such as other forms of coercion, including the seizure of outlying islands, selective quarantines where China restricts traffic to and from Taiwan (e.g. 'inspecting' shipments), or even a full-blown blockade.

Given our deep economic ties with China, including asymmetric dependencies in key sectors, as well as supply chains from Taiwan (in particular in advanced semiconductors), this would lead to a drastic shock causing ripple effects around the world. The EU would face severe disruption in critical sectors, production shortages, and many years of economic and industrial adjustment, as well as mass layoffs and drastically lower living standards[17]. In this regard, **the security and prosperity of the Euro-Atlantic region are closely interconnected with those of the Indo-Pacific**. In light of this, the EU should therefore strive to prepare for, but also to prevent, a major contingency in the Indo-Pacific, working closely with its partners in the region.

Put together, all this forcefully underlines the extremely urgent need for a **stronger EU contribution to European security as part of a rebalanced transatlantic relationship**. Further prioritisation of East Asia by the US for its deployed military capabilities, particularly air and naval capacities on which NATO relies heavily, could leave Europe to face the Russian threat with dwindling US military presence.

15. To provide a snapshot in time, adjusted for PPP, China's 'core' 2024 defence budget would amount to USD 439 billion, while total military expenditure reaches USD 574 billion. This represents a 7.2% increase compared to last year.
See: IISS, China's defence budget boost can't mask real pressures, 2024.

16. See: Bronk, J., Europe Must Urgently Prepare to Deter Russia Without Large-Scale US Support, 2023.
Mölling, C. Preventing the Next War: Germany and NATO Are in a Race Against Time, 2023.

17. Bloomberg's econometric modelling projects a USD 10 trillion cost to the global economy – approximately 10% of global GDP – resulting from even a limited war over Taiwan. This cost is far more than that of the war in Ukraine, the 2008/2009 financial crisis, or even the economic impact of the COVID-19 pandemic.
See: Bloomberg, Xi, Biden and the $10 Trillion Cost of War Over Taiwan, 2024.
According to Rhodium Group, a blockade of Taiwan could endanger well over USD 2 trillion in economic activity, without even considering the impact of international sanctions or potential military responses. This figure should likely be considered a floor rather than a ceiling.
See: Rhodium Group, The Global Economic Disruptions from a Taiwan Conflict, 2022.
See also: Teer, J., Ellison, D., de Ruijter, A., The Cost of Conflict: Economic Implications of a Taiwan military crisis for the Netherlands and the EU, The Hague Centre for Strategic Studies, 2024.

→ The arc of instability and fragility around Europe is widening.

The EU is significantly exposed to its external environment, given its geographical location and its high reliance on external trade for goods and resources, such as energy. It is also **surrounded by growing instability and conflict in its direct neighbourhood** from East to South, often with active interference by Russia and other external actors. This has a range of spill-over effects for the EU, ranging from organised crime and migratory flows, to the blockage of vital maritime routes by non-State actors. War, insecurity, poverty and a lack of opportunities **contribute to displacement within, and irregular migration from the EU's Southern Neighbourhood, to Europe**.

The continuing Hamas-Israeli conflict **in Gaza, strikes between Hezbollah and Israel, as well as the threat of escalation between Iran and Israel** are further **eroding any prospects for peace and stability in the Middle East**. From Northern Africa to the Sahel and the Great Lakes, and from the Horn of Africa to Yemen, security risks are catalysed by **weak States and fragile contexts, entrenched political instability, continued civil wars and ungoverned spaces in which armed groups, organised crime, and foreign interference can flourish.**

Reignited conflicts and spiralling humanitarian consequences continue to plague the region. In Eastern Europe and Central Asia, the potential of frozen conflicts escalating into hot wars remains an ever-present risk. Through its expanding presence of mercenary groups in different parts of Africa, Russia supports military coups and protects illegitimate juntas, instrumentalising fragility while gaining access to mineral and other resources, and increasingly controlling the main migration routes to Europe.

Terrorism in all its forms remains a serious threat to Europe. Recent events have shown that jihadist terrorism has not disappeared, despite the demise of the ISIL caliphate in 2017 – with events in Gaza serving the propaganda and indoctrination efforts of ISIS and Al-Qaeda. Currently, the majority of victims of acts of jihadist terrorism fall in Northern Africa, while Islamist terrorism has also made its mark recently in Russia[18].

There are currently **more ongoing conflicts in the world than at any other point in time since the end of the Second World War** in 1945[19]. There has been a surge in the level of conflict since 2019, even before Russia's war of aggression against Ukraine, including a nine-fold increase in 'internationalised internal conflicts' since 2004[20]. As non-State actors are increasingly using (cheap) drones and may potentially weaponise other technologies as they become more easily accessible (including bio-technology, as the UN warns)[21], conflicts are growing both in scale and in duration[22]. This has enormous humanitarian consequences.

→ Climate change and environmental degradation pose threats to international peace and security.

Climate change and environmental degradation will only further exacerbate instability, the human cost and the potential for internal and inter-State conflict among less climate resilient countries. Extreme weather events, rising temperatures and sea levels, desertification, water scarcity, threats to biodiversity, environmental pollution and contamination and the loss of livelihoods threaten the health and well-being of humanity. In the longer term, natural resource shortages and extreme weather will mean more people are displaced, adding to **the potential for increased migra-**

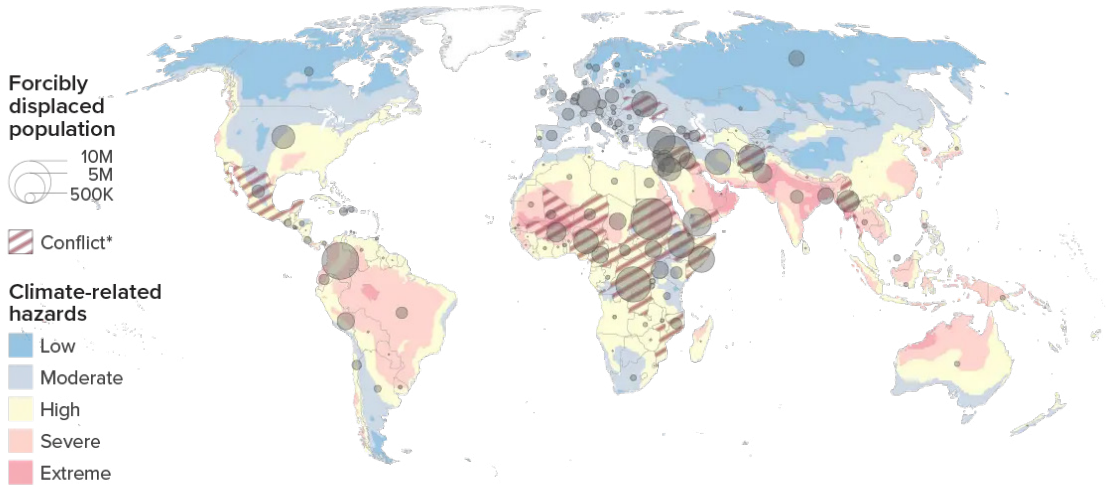
18. Shea, J., ISIL and jihadist terrorism: not the moment the take the eye off the ball, Friends of Europe, 2024.
19. Uppsala Universitet, UCDP: record number of armed conflicts in the world, 2024.
20. Vison of Humanity, Conflict trends in 2023 - Growing Threat to Global Peace, 2023.
21. United Nations, A New Agenda for Peace: Our Common Agenda, Policy Brief 9, 2023.
22. Currently, 56 non-State armed groups are known to possess armed drones. See: Danish Institute for International Studies, Non-state armed groups in the sky, 2024.

tory movements, social unrest, instability and insecurity, and renewed conflicts over scarce resources. Of the 20 countries that are the most vulnerable and least prepared for climate change, 12 were in conflict in 2020[23].

By 2050, it is estimated that more than one billion people will have insufficient access to water, that soil degradation may reach 90%, while demand for food due to demographic trends could increase by 60%[24]. The United Nations High Commissioner for Refugees (UNHCR) estimates that, since 2008 an annual average of 21.5 million people have been forcibly displaced by weather-related events, such as floods and heatwaves. This number is expected to increase in the coming decades[25]. At the end of 2023, almost three-quarters of forcibly displaced people were living in countries with high-to-extreme levels of exposure to climate-related hazards. Nearly half of all forcibly displaced people were living in countries where they remained exposed to conflict, as well as these climate-related hazards. These developments are exacerbated by corrupt or authoritarian regimes, organised crime networks and armed groups that actively instrumentalise **climate and environmentally induced instability and resource scarcity.**

FIGURE 4

Overlap between climate-related hazards, conflict, and forced displacement worldwide (2023)



*Countries with more than one conflict-related death per 100,000.

Source: UNHCR, 2023.

The **melting of Arctic ice** opens new shipping routes and creates new potential for the exploration of fossil fuel and mineral deposits. This has already contributed to **geopolitical tensions as Russia increases its military capabilities in the region**, as manifested by the combat icebreaker project currently in sea trials. In addition, Russia is stepping up its collaboration with China to build infrastructure along the Northern Sea Route. External interest in resources in Arctic locations is increasing,

23. UN Environment Programme (UNEP), Climate Security Mechanism (CSM) Progress Report 2021, 2021. See also Annex 1.

24. See: SIPRI, Environment of Risk: Security in a New Era of Risk, 2022.
World Bank, Groundswell Part 2: Acting on Internal Climate Migration, 2021.

25. In 2023, the Institute for Economics and Peace (IEP) estimated that by 2050, 2.8 billion people will reside in countries facing severe ecological threats, compared to 1.8 billion in 2023, with 1.1 billion of these people living in countries with low societal resilience.
See: IEP, Ecological Threat Report, 2023.

with multi-faceted social, environmental and economic consequences[26]. Globally, climate change has growing geopolitical impact in the maritime domain, both around Europe (e.g. in the Baltic and Black Seas), as well as in the Indo-Pacific.

Moreover, the **energy transition will reshape the configuration of global power** in the decades ahead. It puts a geopolitical premium on the ambition to reduce Europe's external energy dependency, including by harnessing clean energy sources and technologies. This in turn will lead to a **new set of vulnerabilities** linked both to the digitalisation and the decentralisation and greening/electrification of the power supply, connected devices and infrastructure networks (transmission, distribution, storage, etc.). The offshore wind parks in the North Sea have already become the subject of the Russian navy's interest, as neighbouring Member States have warned.

→ The EU and its Member States are targeted by increasingly brazen hybrid campaigns.

Our dependence on modern technologies makes us **vulnerable to cyberattacks27 while our open, democratic societies are vulnerable to malign influence operations, for example in the form of the deliberate manipulation of information**. Russia, China, and other malicious actors actively engage in hybrid operations that prey on such dependencies and vulnerabilities as a 'low cost, high reward' method to achieve their political objectives: driving EU Member States apart and weakening us[28]. **Foreign Information Manipulation and Interference (FIMI)** ranging from disinformation to intimidation is increasingly sophisticated, difficult to recognise or attribute and quickly taking advantage of new technological opportunities[29].

Attacks against critical infrastructure, such as energy grids, can lead to loss of power with effects simultaneously in several Member States, substantial economic damage, and undermined public security. Hospitals whose IT systems are brought down by cyberattacks cannot provide care for patients, have to postpone surgeries or other medical care, potentially endangering human lives. Attacks on water infrastructure by cyber means or through physical sabotage can lead to mass societal panic and catastrophic consequences[30]. We have already witnessed damage to **undersea gas pipelines and submarine communications cables** in suspicious circumstances. Alongside this, the deliberate jamming or spoofing of the Global Navigation Satellite System (GNSS) signals affects aviation safety.

As hundreds of Russian intelligence officers operating under diplomatic cover have been expelled from EU Member States, **Russia seems to be increasingly turning to proxies to carry out its sabotage operations**, targeting for example critical transportation links, commercial properties, water management systems and military warehouses that are used to provide support for Ukraine. Increasing sabotage and other hybrid operations may start to **undermine citizens' sense of security**, as well as the economic attractiveness of the countries most aggressively targeted. Reckless tactics, including arson and the use of explosives, pose serious risks to public safety.

26. European Commission and High Representative, Joint Communication on a stronger EU engagement for a peaceful, sustainable and prosperous Arctic (JOIN(2021) 27), 2021.

27. ENISA, ENISA Threat Landscape 2023, 2023.

28. According to the European Centre of Excellence for Countering Hybrid Threats, hybrid threats or campaigns describe coordinated and synchronised actions that deliberately targets democratic States' and institutions' systemic vulnerabilities using a wide range of means. Hybrid activities actively exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-State, and national-international). Primarily, they aim to influence different forms of decision-making at the local (regional), State, or institutional level, and are designed to further and/or fulfil the agent's strategic goals, while undermining and/or hurting the target.
See: European Centre of Excellence for Countering Hybrid Threats, Hybrid threats as a concept, 2024.

29. While rooting out disinformation and misinformation is practically impossible in democratic societies with open information spaces, it is evident that these operations are less effective in societies with high levels of social cohesion, media literacy and trust in the fairness of the political system and public authorities in general.
See for instance: Dragomir, M., Rúas-Araújo, J., and Horowitz, M., Beyond online disinformation: assessing national information resilience in four European countries, Humanit Soc Sci Commun 11, 101, 2024.

30. In January 2024, FBI Director Christopher Wray publicly warned that Chinese hacker groups were preparing to target and disrupt US critical infrastructure.
See: CNN, FBI director warns that Chinese hackers are preparing to 'wreak havoc' on US critical infrastructure, 2024.

At the same time, public institutions such as universities, public administrations, ministries, but also private companies in the digital sector, including start-ups and SMEs have been **targets of cyberattacks** by actors linked to China and Russia.

The functioning of our economy from the level of individuals to the EU as a whole depends on a reliable payments transaction system. Even a short interruption or breach of confidentiality of financial data would have **broad societal and economic consequences**. In addition to malicious State actors, our financial system remains a frequent target of cyberattacks and ransomware by criminals seeking financial gain.

The instrumentalisation of migrants is part of hybrid operations, including by Belarus and Russia, but also other countries to the south and south-east, to put pressure on EU Member States at the EU's external borders. They aim to create a sense of insecurity and to polarise societies, to decrease citizens' trust in public authorities and take advantage of loopholes in legislation and international law, such as the 1951 Refugee Convention.

Violent extremism inside Europe by radical political movements and individuals poses a threat to public security and has already resulted in riots, assassinations and other organised acts of violence. Some external actors seek to breed these internal grievances, the desire for retribution and vengeance. Supporting recruitment, radicalisation and the mobilisation to violence, including terrorism, is another way in which societal discontent is weaponised against us.

→ The economy and security have become increasingly intertwined.

Great powers have always competed for technologies and economic supremacy as a way to gain strategic and military advantages. What is different now is that as a result of the post-Cold war era of rapid globalisation, Europe's economy, societies and even militaries have come to critically depend on globalised supply chains. **In a world of growing resource scarcity and an increased risk of weaponisation for (geo)political purposes, trade, technology, energy and raw materials are increasingly drawn into security and strategic dynamics.**

Adversarial powers are already anticipating and adapting, often pursuing a more aggressive de-risking policy than we are. China has stepped up its focus on assertively enhancing **the resilience of its industrial and supply chains** – including to sanction-proof its economy, strengthen and expand its strategic stockpiles, as well as to develop China's strategic hinterland and ensure backup plans for key industries; and on **reaching scientific and technological self-reliance from Western countries**. China's persistent macroeconomic imbalances, along with its non-market policies and practices, are generating overcapacity that, if allowed to flood with no restraint foreign markets, advances the country's stated ambitions to dominate key industrial sectors. Combined with China's increasing use of economic interdependence as a tool of coercion, this **threatens to undermine Europe's long-term prosperity and security**, while granting China a significant strategic advantage over time.

More broadly, the EU needs to face the reality that other global powers consider their industrial performance, trade and technological innovation as instruments of statecraft. Europe has recently experienced economic coercion by foreign powers; the weaponisation of energy dependency following Russia's war of aggression against Ukraine; economic espionage and technology leakage; foreign direct investments posing possible security risks for Europe in EU-based companies; and the dumping of Chinese industrial overcapacity in critical sectors for the future, such as electric vehicles and clean technologies. The EU's **economic security strategy** should be further consolidated and expanded to address links to the defence industry, critical infrastructure and hybrid threats.

By their nature, **large scale crises – even at vast distances – have the potential to severely disrupt the flow of essential goods and services**, impacting the very foundation of economic and societal stability. These risks can be mitigated by de-risking problematic dependencies through supply chain diversification, 're-shoring' and including economic security standards in regulatory frameworks and

(public) procurement policies. The resilience of the EU's economy and societies, especially **in sectors critical for maintaining societal and economic stability,** such as food, health, drinking water and wastewater, energy, transport, public administration, education, banking, financial market infrastructures, digital infrastructure, and space, is paramount in face of potential large-scale crises, such as military conflicts and disasters.

Geopolitical tensions highlight the risks of **serious disruption to global supply chains** and the EU's access to critical raw materials and commodities, such as foodstuffs, medical supplies, fertilisers, energy, and components needed in **critical defence and civilian sectors**. Many of these risks and shortages have recently materialised in connection to the COVID-19 pandemic, Russia's full-scale invasion of Ukraine and, for example, the attacks of Houthi rebels against Western vessels in the Red Sea. Measures to reduce economic vulnerabilities through preparedness actions will need to complement the 'just-in-time' principle on which our globalised economy has been based, driving new trade-offs between cost-efficiency and preparedness considerations.

Combined with the **multiplying effects of climate change and the digital transition**, the EU needs to anticipate that current competition for resources, technologies and economic strength will only further intensify and broaden – and with it the potential for intentional or unintentional disruptions. The scramble for natural resources and raw materials will continue to shape strategic competition and international relations in particular between major economies and the so-called 'Global South'.

→ The race to control disruptive technologies will intensify.

Disruptive technologies can shift economic performance to a higher level. Controlling them can add to the arsenal for power and global influence. The pace of innovation, spurred on by AI-enabled technologies, will only further rise. Disruptive technologies offer untold possibilities, but also come with **new vulnerabilities and security concerns**. Unmanned air and naval systems, enabled by artificial intelligence, will further **change our societies as well as the nature of warfare**. Quantum computing can set off a new wave of innovation, while posing severe risks to encryption keys used worldwide.

In particular in view of geopolitical confrontations, the EU needs to be more resilient and to minimise **external dependencies in critical sectors that are vital for society in crisis situations.** This requires the EU to focus even more on **regaining and strengthening its innovative and competitive edge**, while stepping up its work to enhance supply chain resilience and to de-risk unwanted dependencies. The Union needs to protect its science and technology potential and **safeguard its ability to access, develop, operate, control, produce and secure critical goods and technologies, including those related to military capabilities.**

Conclusions

This overview of the main geopolitical, climatic, economic and technological risk drivers in the previous chapter shows that **Europe requires both urgency and agency** to face them collectively and effectively, working together at all levels:

- **Urgency:** Despite the many wake-up calls and warnings during the past years, there is still an urgent need to **strengthen our collective action and to overcome years of neglect, underinvestment and fragmented efforts**. The gap between the threat level and our preparedness will only widen further, unless we start better anticipating the wide range of risks we face and take bold and comprehensive action today. There is an immediate need to raise the awareness of our citizens of current and future risks, combined with a positive agenda of how we can work together to prepare for these challenges.

- **Agency:** The EU is the world's largest trading bloc and an important security and defence actor with a broad **arsenal of tools to protect its citizens**. This provides the basis for an enhanced ability to prevent, cope with, and respond to even the most serious threats. The EU must also be able to meet the expectations of its citizens, who consider providing security as an increasingly important priority for the Union. Working together as Europeans is the only way to positively shape our regional and strategic order, and our Union's global future.

As always, Europe's shift to a higher level of preparedness, including for the threat of armed aggression, ultimately depends on the **political will, commitment and concerted efforts of Member States.** In this regard, the risk and, alas, too often the reality of short-termism and diverging interests, security priorities and political views hampering joint actions and investment remains real, in particular considering the polarised societal and political landscape across Europe.

CHAPTER · CHAPTER · CHAPTER

02

Enabling the EU to function under all circumstances

Introducing comprehensive preparedness

Against the challenging risk landscape and crisis-prone world set out in the previous chapter, **the primary objective of preparedness is to 'crisis-proof' the ability of the European Union and its Member States to uphold vital governmental and societal functions**. The EU as a whole must be able to function under all circumstances in order to take and implement decisions and actions that protect EU citizens in times of crisis. In a similar vein, the EU's preparedness must cover the full range of threats and hazards, from extreme weather events to State-sponsored interference and, in the most extreme instance, armed aggression against one or more of our Member States. This reflects the call by the European Council, in its March 2024 Conclusions for enhanced and better coordinated crisis response at the EU level, adopting a whole-of-society approach which takes into account all hazards[01].

In this context, 'comprehensive preparedness' refers to the ability of the EU and its Member States to **effectively anticipate, prevent, withstand or respond to any type of major shock or crisis with cross-sectoral and cross-border impacts, and which can even threaten the EU as a whole**. The overarching aim should be to ensure that the EU and its Member States can continue to **function under all circumstances. This full-spectrum preparedness challenge lies at the heart of this report.**

A comprehensive perspective on preparedness needs to take into account that different threats pose distinct challenges to the Union's ability to function under all circumstances: In the event of armed aggression or, for example, a devastating large-scale cyberattack, there is an immediate risk of a serious disruption to the continuity of critical functions. On the other hand, climate change continually degrades the EU's ability to function in the long term, for instance by exacerbating

01. European Council, European Council meeting (21 and 22 March 2024) - Conclusions, 2024.

increasing shortages and irregularities in the supply of critical resources, such as food and clean water, increasing the risk of new pandemics, and fuelling increasingly intense and frequent disasters and extreme weather events. Despite their different nature (e.g. 'looming' and 'acute', versus 'creeping' threats), these threats are also cumulative in nature and mutually reinforcing (as set out in chapter 1), thus creating a number of horizontal challenges that need to be addressed in an integrated way.

The starting point for building comprehensive preparedness is that the EU currently lacks an agreed, comprehensive list of the vital societal and governmental functions which we must be able to protect at all costs. Such vital functions include in particular the protection of the EU's decision-making capacity – starting from the highest political level. The EU must be able to support Member States in the provision of citizens' basic needs (e.g. food, water, housing and shelter, protection, health and sanitation), as well as ensure the continuity of its essential services and functions, such as the Single Market, public order and security, energy, transport, telecommunications and digital services, border management, economic and financial management, and satellite-based services.

These governmental or EU functions not only ensure the smooth running of our societies and economies, but are also critical enablers that allow civilian and military crisis responders to operate effectively in crisis situations. Therefore, integrating civilian/military and 'dual-use' functionalities in all relevant policies is one of the fundamental areas of further improvement considered in this report. The following chapters will develop this aspect in more detail.

For each of these functions, the EU already disposes of a wide array of sectoral frameworks, legislation, and mechanisms that all contribute to different dimensions of preparedness. Ranging from civil protection, climate mitigation and adaptation, migration and border management, and consular protection to health security, food security or organised crime, coordinated mutual support and joint initiatives are a core part of EU action. To name just a few notable legislative and other initiatives adopted during the past mandate, the EU has significantly advanced its crisis preparedness by:

- **Establishing a strong health crisis preparedness and response framework**, which builds on two cornerstone legislations – the Serious Cross-Border Threats to Health and Emergency Framework regulations. The former reinforces overall preparedness, surveillance, early warning and response capacities, including by codifying the possibility to formally recognise a public health emergency at Union-level and calling for the development of a Union Prevention, Preparedness and Response Plan. The latter establishes a framework for ensuring the supply of crisis-relevant medical countermeasures in the event of a public health emergency at Union level, including through Union-level procurement on behalf of Member States.

- **Adopting a New Migration and Asylum Pact, which will enhance migration preparedness** and response. In particular, the new Asylum and Migration Management Regulation establishes a mandatory but flexible system of solidarity for Member States facing migratory pressure and the Crisis and Force Majeure Regulation provides for enhanced solidarity and for a range of procedural derogations to react to crisis situations of crisis, including instrumentalisation [see also chapter 6], and force majeure.

- **Strengthening all-hazards disaster management capacity** by establishing the first-ever EU level strategic reserve – rescEU. Complementing Member States' capacities under the Civil Protection Pool, rescEU hubs spread across 22 Member States and Union Civil Protection Mechanism Participating States provide around 50 emergency response capacities, including a fleet of firefighting planes, CBRN equipment and countermeasures, generators, transport and logistics equipment, shelter, Emergency Medical Teams and medical stockpiles as well as other items.

- **Developing a contingency plan for ensuring food supply and food security in times of crisis**, which included the creation of the European Food Security Crisis preparedness and response Mechanism (EFSCM). The EFSCM provides a forum to monitor the state of food security and supply and provide preparedness- and response-related recommendations.

- **Adopting the Internal Market Emergency and Resilience Act (IMERA)**, which provides a major contribution to the EU's overall crisis preparedness from a Single Market perspective. IMERA enables the activation of crucial coordination and emergency response measures to keep the Single Market and it supply chains functioning during a crisis. For instance, this includes supply chain monitoring for critical goods, measures to ensure free movement inside the EU (including a prohibition on intra-EU export restrictions of critical goods), information requests and priority-rated requests to companies, Commission-led public procurement, placing of critical products on the market, and recommendations to companies to repurpose or expand their production capacities.

In addition, evidence suggests that Member States and communities across the Union have slowly but steadily increased their coping capacity in the face of disasters[02] over the past decade. According to the European Commission Joint Research Centre's Vulnerability Index[03] which – as part of the wider Risk Data Hub – measures vulnerability to disasters – both natural and human-induced – across different administrative levels[04], European countries appear to have steadily decreased their vulnerability by gradually reinforcing their coping capacity, resilience and ability to deal with adverse events. Nevertheless, the 'hazard-independent' Vulnerability Index does not by itself take into account the EU's increasingly complex and rapidly evolving threat environment. In other words, the shifting magnitude of threats and our growing risk exposure poses growing challenges to our ability to cope and poses new demands for the future.

While respecting ongoing efforts to enhance preparedness in different sectors, this report therefore puts emphasis on **horizontal and strategic crisis management, as well as cross-sectoral preparedness**. To ensure the EU's ability to operate under all circumstances, we cannot work in silos. Different vital functions are mutually reinforcing. We face an urgent imperative to connect all individual efforts to the wider work on strengthening the EU's long-term resilience.

This requires us to **further review and strengthen our institutional and regulatory set-up and to scale-up our level of preparedness and readiness**, taking into account all relevant sectors and major contingencies. This entails, for example:

- Better 'connecting the dots' between sectoral mechanisms and instruments to ensure effective coordination and information sharing and avoid siloed approaches. Mapping the potential linkages and cascading effects in crisis situations is an important step in this regard.

- Making sure that essential (cross-)sectoral EU instruments and standard operating procedures are in place before a crisis hits and are designed in a way to enable crisis responders at the EU level and in Member States, rather than becoming obstacles.

At the start of the pandemic, we were caught off-guard, but still managed to accelerate our action rather quickly. We may not always have that luxury. Ensuring the EU's ability to function under all circumstances therefore means **taking worst-case scenarios seriously as the benchmark for our preparedness efforts.** This applies to the main risk drivers: climate change, technology and digitalisation, as well as the security and defence context – as further developed below.

02. Disasters can be defined as natural or human-induced adverse events that cause devastation of human life, property, environment and cultural heritage.

03. Risk Data Hub: An online platform for risk assessment across the EU, publishing data on regional hazards, vulnerability, and risk levels.

04. The Vulnerability Index builds on more than 100 open-source indicators clustered around five dimensions (economic, environmental, physical, political, and social) to approximate communities' vulnerability and coping capacity at both the regional and national levels.

Enhancing preparedness for worst-case climate scenarios

Seen through a preparedness lens, climate adaptation and steps to enhance our long-term security should increasingly be considered as part of the same resilience-building challenge for Europe. Both require a whole-of-government and whole-of-society approach, and ultimately draw on limited natural and financial resources. We therefore need an approach that connects the two, rather than treating them as competing priorities. Both also require us to look ahead at the world in one or two decades from now for the design of investment strategies and capability development efforts.

Even in a best-case scenario where we limit global warming to 1.5 degrees above pre-industrial levels, Europe – which is heating at twice the global rate – will have to learn to live with the consequences of a climate that is 3 degrees warmer or even more[05]. Moreover, while striving to achieve the European Green Deal's ambition of climate-neutrality by 2050 with determination, we need to be realistic about the growing set of climate risks, as outlined in chapter 1. **To accelerate the implementation of ambitious and cross-cutting climate adaptation policies, the latter should use a reference climate scenario corresponding to 3 or more degrees above pre-industrial levels.** As outlined in the Political Guidelines (2024-2029), the upcoming European Climate Adaptation Plan should outline the necessary steps forward in this regard.

Ensuring climate resilience across our economy, society and infrastructure is vital to maintain core societal functions in light of the full range of climate risks, including more extreme weather events that may get progressively worse. Forest fires combined with droughts, floods, but also lower water levels in the river system due to melting mountain glaciers.

The EU's climate adaption policies will also need to integrate wider security and geopolitical challenges – ranging from de-risking supply chain dependencies to the security of future energy infrastructure, and the energy transition of the defence sector. Moreover, climate change, environmental degradation and ecological change are slowly transforming and shifting the natural resource base on our continent and globally. Warming twice as fast as others, Europe is facing a gradual redistribution and contraction of natural resources, species and ecosystems. Water stress and soil degradation in the EU already have negative effects on crop and food production, drinking water supplies and energy generation.

Moreover, without meaningful action to slow down or reverse the loss of Europe's climate and ecological niche, the EU may end up developing new dependencies for a range of foundational resources. Shortages in these areas may become an acute deficiency at times of geopolitical confrontations. Ecological change and resource scarcity at the global level is also likely to spark international crises and spill-over to the EU [see also chapter 8]. Rethinking resource management therefore has clear implications not only for our well-being and prosperity, but also our long-term security. Thus, preserving our ecological carrying capacity is at the core of Europe's preparedness challenge.

In this vein, tackling unsustainable land use and the structural mismanagement of water, or strengthening the circularity of Europe's economy, are all pieces of the puzzle to ensuring the EU's functioning under all circumstances. Also in this regard, the EU and Member States can further build on different policies put in place. For instance, under the Critical Entities Resilience Directive, Member States have an obligation to take specific actions to increase the resilience of water supply and wastewater entities. The proposal for a Soil Monitoring Law aims to promote monitoring and to improve soil health. Under the EU Circular Economy Action Plan, the Union has launched several regulatory initiatives to promote the transition to a more resource-efficient, and at the same time, more resilient economy. Nevertheless, more needs to be done. In this regard, the announcement of a future European Water Resilience Strategy as part of the Political Guidelines (2024-2029) sends an important signal. Preserving access to clean and affordable freshwater, as well as other foundational resources – both within and outside the EU – needs to remain a guiding priority.

05. European Commission, Communication on Managing climate risks - protecting people and prosperity, 2024.

Enhancing the EU's preparedness for a major cyberattack

Increased the digital connectivity of our societies and economies means **a bigger cyberattack surface, as well as greater possible repercussions throughout the grid** (and the services it connects) if the right cyber protection measures are not implemented. Malicious cyber activity against the EU and numerous targets across the Union has for years been a daily reality. Evermore serious cyberattacks are a growing threat to critical infrastructure with the potential to escalate into a crisis. Authoritarian States continue to behave irresponsibly in cyberspace and often use proxies to launch ever more sophisticated intrusions aiming to steal data, disrupt or destroy vital economic and societal components. Attacks against **energy grids** can lead to a loss of power and substantial economic damage. **Hospitals** which fall victim to attacks cannot provide care for patients, have to postpone surgeries or other medical care, potentially endangering lives. Attacks on **water infrastructure** can lead to mass societal panic or catastrophic danger if the attack targets dams. Attacks on **banks** can lead to a disruption of financial services, even potentially impacting their liquidity. Attacks on **transport providers** or infrastructure (air controllers, railways, ports, etc.) could cause chaos around Europe and beyond. And an attack on the **armed forces** could render their capabilities temporarily inoperable.

Such cyberattacks alone would be devastating, but could also be used as part of a wider hybrid or military confrontation, or as part of coercive strategies to affect the EU's strategic or diplomatic position. Against this backdrop of an extremely dynamic threat landscape and a constantly contested cyberspace, a number of further actions are needed to ensure the preparedness and resilience of the EU. The EU has made major strides forward in recent years[06], but there is still room and a growing need to go further. Given the broad cross-sectoral effects of a major cyberattack, cybersecurity and resilience need to be integrated into a whole-of-government approach to ensure better operational coordination between civilian and military cyber actors and across sectoral crisis management mechanisms in the fields of energy, finance and healthcare, for example. Improved trust between the public and private sectors is needed to share information on cyber threats and to detect them earlier, taking advantage of the European Cybersecurity Alert System. The various new Commission cyber capabilities – the recently inaugurated Cyber Situation and Analysis Centre – need to fit into an already wide range of relevant bodies, platforms and activities, while also ensuring docking points with other crisis response actors more horizontally [see chapters 2 and 3]. Revisiting the Cyber Blueprint (2017) would provide an opportunity to streamline and identify trigger points for whole-of-government preparedness, including in the view of worst-case scenarios.

Enhancing EU preparedness for major military contingencies

Any serious reflection on comprehensive preparedness must cover the possibility of a major military crisis triggered by external armed aggression against one of the Union's Member States. This scenario has already been recognised among the main disaster response scenarios and certain aspects were exercised as part of the recent Parallel and Coordinated Exercise (PACE) with NATO in 2024. Armed aggression through conventional means may be accompanied by other hostile activities, such as very serious hybrid operations, cyberattacks or the use of chemical, biological, radiological or nuclear weapons.

Yet, the scenario has not been fully developed and mapped out within the EU framework as such. **The shift to comprehensive preparedness requires us to assess the full scale of societal, economic,**

06. Notable examples include the NIS2 Directive, the Cyber Solidarity Act, or the Cyber Resilience Act.

security and other implications of any armed aggression against one of the EU's Member States – and which measures to put in place to be prepared for them. It should link to the 'European Civil Defence Mechanism' envisaged in the Political Guidelines, given the legal definition of civil defence under international humanitarian law[07].

The EU needs to be prepared to use all the tools at its disposal to support the Member State that is under attack. With 23 out of 27 Member States being part of NATO, which remains the backbone of the collective defence of its members, **there is an inherent EU-NATO dimension here. The Union would be heavily impacted and involved in the event of an activation of Article 5 of the North Atlantic Treaty, even if there is no automaticity in this regard**. NATO requests to the EU for support would require appropriate decision-making, taking into account the principles of the autonomy of decision-making of each organisation, inclusiveness of all Member States and respect for the security policy of all Member States.

Yet, politically and practically, if such a flagrant violation of our territorial integrity were to manifest itself, with all the disastrous consequences for the citizens on the frontline, as well as the economic havoc that would ensue, **the EU itself would be engaged in a crisis mode of the highest order**. In fact, the attacked Member State could well invoke the Mutual Assistance Clause of the EU Treaties (Art. 42.7 TEU), alongside any invocation of Article 5 of the North Atlantic Treaty. **In any event, the EU needs to be better prepared for this most extreme crisis from a European perspective, in coherence and complementarity with NATO.**

There are many possible areas in which the EU would be engaged in such a scenario: notably through its competences related to diplomacy, enacting (emergency) legislation, sanctions and other retaliatory measures, transport, civil protection assistance to refugees and other affected populations, health and medical support, defence industrial readiness, countering hybrid threats, protecting critical infrastructure, border protection, law enforcement, ensuring secure communications, providing economic and financial assistance and/or military training and assistance, ensuring the continuity of the workforce, maritime safety and security measures, Single Market resilience, etc. Moreover, in a multifront scenario in which military tensions in the Taiwan Straits or South China Sea escalate at the same time, we need to expect major disruptions of critical supply chains alongside intensifying competition for influence and access to resources in (non-aligned) third countries.

In fact, several services of the Commission, together with the EEAS and the European Defence Agency (EDA), are already working with NATO counterparts on resilience, enablement and preparedness questions in different sectors. The most prominent example is the EU initiative on **Military Mobility**, which is ultimately driven by Member States' defence needs (defined by NATO in more detail) to move large-scale forces at short notice for crises at our external borders and beyond [see also chapter 7]. Other Commission services are engaged in EU-NATO dialogues related to CBRN preparedness, including in view of the possible need for mass evacuations, or in stepping up the back-up of **medical supplies and preparing hospitals for mass casualties**.

Further work at the EU-level needs to take into account that NATO allies are enhancing their whole-of-government preparedness for armed attack, in line with Art. 3 of the North Atlantic Treaty[08], through the implementation of seven Resilience Baseline Requirements[09]. NATO members use a set of more detailed implementation criteria and resilience guidelines to assess and improve their national resilience in view of armed attack, and report back to NATO on their efforts. **Many if not all of these areas are governed and regulated by EU policies, tools and instruments, at**

07. European Commission, Europe's Choice – Political Guidelines for the next European Commission 2024-2029, 2024.

08. Article 3: 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack'.

09. 1) the Assured Continuity of Government and Critical Government Services; 2) Resilient Energy Supply; 3) Ability to deal with Uncontrolled Movement of People; 4) Resilient Food and Water Resources; 5) Ability to deal with Mass Casualties; 6) Resilient Civil Communication Systems; and 7) Resilient Civil Transportation Systems.

least for the Member States concerned. This raises the importance of coherence and synergies between NATO policies and EU legislation and funding instruments in these areas, which is being addressed through different sectoral dialogues between EU and NATO staff. We do have to bear in mind, of course, that **the primary objective of relevant EU policies is much broader**.

That said, **further work is required to assess the intersection between NATO's work on these baseline requirements (and the wider enablement and other policies) and relevant EU policies, tools and instruments.** The scope of involved EU policies and instruments still needs to be defined more comprehensively in the EU framework, based on a whole-of-government vision to be articulated for this type of extreme scenario. There are subsequently different levels at which the EU and NATO would intersect:

- At the operational level, it is important to identify – to the extent possible – civilian and military coordination points ('who does what') including when EU-level actors would need to be engaged in support of the Member State concerned or as part of wider EU mechanisms that may be applicable in this context. Moreover, possible resource and access challenges should be identified.

- At the policy level, it will be key to ensure coherence and mutual reinforcement between respective policy developments where appropriate and relevant, while preserving the autonomy of EU-decision-making and respecting the primary objectives of relevant EU policies. Further improving information sharing and staff-to-staff dialogue will be critical in this regard. Synergies and links between national reporting and assessment processes within NATO as regards the baseline requirements with and between relevant EU-level mechanisms would need to be further explored.

In short, the EU's range of whole-of-society policies and tools, and related regulatory and financial powers, would be indispensable in an 'Article 5 situation'. **However, the EU itself has yet to define a coherent vision in this regard, as the possibility of war against an EU Member State has for long been regarded as too politically sensitive and potentially divisive.** This can no longer be the case. As part of an all-hazards or comprehensive preparedness approach, concrete scenario-based thinking must connect the dots between different EU work strands and their connections with NATO. **In today's security environment, EU preparedness can only be credible if it covers this fundamental threat.**

Recommendations

1. **Develop a comprehensive EU Risk Assessment to help identify the major cross-sectoral threats and hazards as well as the concrete risks facing the European Union as a whole, building on current sector-specific risk assessment processes.**

2. **Use the upcoming Preparedness Union Strategy to put the EU on track for comprehensive preparedness.**
   - × Define at EU level vital societal and governmental functions, for which continuity needs to be ensured.
   - × Develop EU-level Preparedness Baseline Requirements for each of the identified vital functions.
   - × Ensure the coherence and alignment of sectoral crisis plans and blueprints at the EU level.
   - × Embed a 'Preparedness by Design' principle horizontally and consistently across EU institutions, bodies, and agencies and develop a mandatory 'Security and Preparedness Check' for future impact assessments and 'stress-tests' of existing legislation.
   - × Explore the feasibility of an EU Preparedness Law, setting joint standards and long-term guidelines, aligning EU and national efforts wherever possible.

3. **Set up and regularly conduct an EU Comprehensive Preparedness Exercise horizontally testing both high-level decision-making and operational coordination and building strong links between actors and across sectors.**

4. **Articulate a coherent vision for the EU's role – within its competences – in preparing for and responding to an Article 5 activation in the event of armed aggression against an EU Member State, by mapping the full-scale of implications and linking different sectoral work strands.**

5. **Strengthen the EU-NATO interface in view of potentially grave crisis situations, including through an emergency protocol that can be activated to streamline information exchange.**

1. DEVELOP A COMPREHENSIVE EU RISK ASSESSMENT.

To better manage risk, prepare for crises, and enhance the safety and security of our citizens, the EU needs a thorough and comprehensive all-hazards and all-threats risk assessment, covering all sectors of the EU's activities. Member States already submit general national risk assessments under the Union Civil Protection Mechanism, as well as in certain sectoral domains. The EU Overview of Risks[10] summarises the common trends, but is limited to non-confidential information and is exclu-

10. Union Civil Protection Knowledge Network. EU Overview of Risks. 2024.

sively focused on disaster risks. To step up the EU's preparedness, an enhanced and comprehensive risk assessment process should be developed, drawing on national risk assessments and sectoral risk assessments at the EU level, such as the EU Climate Risk Assessment[11], the Health Emergency Preparedness and Response Authority's (DG HERA) annual Threat Prioritisation exercise, as well as the Threat Analysis done by the Single Intelligence Analysis Capacity (SIAC) in the context of the Strategic Compass.

The comprehensive EU Risk Assessment should bring together natural hazards and security threats by addressing both the EU's evolving geopolitical environment and the role of climate change as a risk driver and multiplier, taking into account cross-border risks, interdependencies and possible cross-sectoral cascading effects. The risks identified would then serve as a basis for decision-making, preparedness planning, and actionable risk management measures. To this end, Commission services and the EEAS should cooperate closely with Member States to harmonise – to the extent possible – national and sectoral methodologies, to align timelines, and smoothen out potential duplications.

2. USE THE UPCOMING PREPAREDNESS UNION STRATEGY TO PUT THE EU ON TRACK FOR COMPREHENSIVE PREPAREDNESS.

During the current institutional cycle, the EU has developed important strategies across several domains, such as the Strategic Compass for security and defence, the European Security Union Strategy, the Economic Security Strategy and the Global Health Strategy. The Political Guidelines for the next mandate (2024-2029) further build on this work, proposing a White Paper on the Future of European Defence, an Internal Security Strategy, and a Preparedness Union Strategy. The envisaged Preparedness Union Strategy should make concrete proposals to align and coordinate implementation between these overarching strategies, 'connecting the dots', and, where necessary, propose complementary measures to strengthen the EU's preparedness as required. The European Council should be enabled to provide strategic guidance. Timely decision-making in response to evolving threats should be ensured by the EU institutions, in line with their prerogatives under the Treaties.

→ Define at EU level vital societal and governmental functions for which continuity needs to be ensured.

As part of the forthcoming Preparedness Union Strategy, this should include defining the necessary measures to ensure the EU's own decision-making and implementation capacity so as to be able to act in the most severe crises and ensure the 'continuity of government' in the EU institutions. To that end, building on and complementing existing legislation, the EU should determine the sectors most critical to providing essential services to citizens (e.g. food, clean water, access to healthcare), as well as those ensuring the continuity of core governmental and economic functions – and the critical dependencies between them. This also requires identifying functions that are critical enablers for civilian and military crisis responders (e.g. secure communications, transport, intelligence, surveillance and reconnaissance, earth observation and global positioning). For the latter, the strategy should also define corresponding capability targets to guide future investments in infrastructure and capability development, as well as research and innovation.

→ Develop EU-level Preparedness Baseline Requirements for each of the identified vital functions.

Ultimately, these critical services and functions need to be highly resilient to shocks and capable of enabling civilian and military crisis responders while keeping the whole of society and the economy running under any circumstance. For each of the vital functions identified, clear overarching baseline requirements should be developed to guide future preparedness work. These preparedness baseline requirements should draw on the findings and recommendations set out in this report,

11. European Environment Agency. European Climate Risk Assessment. 2024.

subject to further discussion and assessment, in view of the full spectrum of threats. They could reflect or incorporate the EU's Disaster Resilience Goals, as well as the hybrid resilience baselines developed under the Security Union Strategy. In relevant sectors, alignment with NATO's resilience baselines should be promoted, while noting that the EU's baseline requirements are defined on a broader set of risks than in NATO and potentially involve a wider set of sectors and stakeholders – reflecting the EU's comprehensive role.

→ Ensure the coherence and alignment of sectoral crisis plans and blueprints at the EU level.

The new Preparedness Union Strategy should pave the way for an alignment of all the different sectoral blueprints and crisis plans[12] from a whole-of-government and comprehensive preparedness perspective. Ensuring coherence and consistence between sectoral blueprints is key to streamlining cross-sectoral action at EU level as much as possible and providing – to the extent possible – clear answers to the many 'who does what' questions that may arise depending on the scenario.

Revising and aligning sectoral blueprints and crisis plans, including the upcoming Union Prevention Preparedness and Response Plan for health crises, requires clarifying roles and responsibilities, further coalescing the EU's crisis management architecture, and linking all those involved – from citizens and private entities to civil and military actors; and from European and national to local and regional authorities, fully respecting the competence of Member States on national security. As such, this would also contribute to the reflection on a possible future EU Preparedness Law. Building on this review and alignment process, the EU could also explore the need for an overarching and high-level EU crisis blueprint, specifically covering the horizontal, cross-sectoral dimension of EU crisis management.

→ Embed a 'Preparedness by Design' principle horizontally and consistently across EU institutions, bodies, and agencies and develop a mandatory 'Security and Preparedness Check' for future impact assessments and 'stress-tests' of existing legislation.

The Political Guidelines' (2024-2029) call for the assessment of policies through a 'security lens' and the integration of security into EU policy-making by design. In line with this as well as building on the existing 'Do No Significant Harm' principle and the climate mainstreaming approach, the Preparedness Union Strategy should establish a 'preparedness by design' principle at its core. Rather than treating security or climate considerations separately or establishing them as competing or mutually exclusive priorities, this principle should address both man-made and natural threats (including climate risks) and contribute to mainstreaming a consistent and horizontal culture of preparedness across EU institutions, bodies and agencies.

Integrating a corresponding mandatory 'Security and Preparedness Check' in the Better Regulation Toolbox should ensure that horizontal security and preparedness considerations are meaningfully taken into consideration as part of the impact assessments for future legislative proposals and reviews.

In addition, as a holistic tool, such a 'Security and Preparedness Check' could also be applied in the context of the upcoming stress-test of the entire EU acquis with a view to simplification. The check could ensure that any review of existing legislation identifies possible regulatory bottlenecks undermining the EU's crisis preparedness.**Explore the feasibility of an EU Preparedness Law to set joint standards and long-term targets, ensuring coherence with Member States' national activities.**

12. Notable examples include the Cyber Blueprint (2017), the Migration Preparedness and Crisis Blueprint (2020), the contingency plan for food supply and food security (2021), the contingency plan for transport (2022), the EU Critical Infrastructure Blueprint (2024), or the EU Hybrid Toolbox for a coordinated response to hybrid campaigns (2022).

To implement the Preparedness Union Strategy, the EU could explore the feasibility of enacting a Preparedness Law setting uniform preparedness standards and measurable targets. This would ensure joint European ownership, with the European Parliament and the Council jointly agreeing on principles, standards, and targets that will guide crucial EU preparedness efforts. In doing so, it would ensure the involvement of Member States in the process. In addition, to improve the EU's capacity for coordinated and swift crisis response, there should be a systematic streamlining of decision-making, coordination, and information-sharing processes, as well as further clarification of the roles and responsibilities at the EU, national, and local levels. Full alignment and complementarity with relevant sectoral legislation should be ensured.

3. SET UP AND REGULARLY CONDUCT AN EU COMPREHENSIVE PREPAREDNESS EXERCISE TO TEST HIGH-LEVEL DECISION-MAKING, OPERATIONAL COORDINATION AND TO BUILD STRONG LINKS BETWEEN ACTORS AND ACROSS SECTORS.

Preparedness measures need to be comprehensively and horizontally exercised. The Union should therefore design and regularly conduct an ambitious EU-wide Comprehensive Preparedness Exercise that tests both high-level decision-making and operational coordination elements and reinforces links between all actors – including, where appropriate, the private sector, civil society, and international partners – and all fields of the EU's activities. This new exercise concept should be built upon the many years of experience of operational and table-top (decision-making) exercises spanning different sectors and actors – including multi-dimensional civil protection and military exercises and the multi-layer Integrated Resolve exercise conducted every two years in the conceptual framework of the 'Parallel and Coordinated Exercises' (PACE) with NATO.

Scenarios should be multi-dimensional and build on the results of the all-hazards and all-threats EU Risk Assessment, as well as other relevant scenarios already identified under the Union's Disaster Resilience Goals[13]. To ensure clear added value, the exercise needs to result in a meaningful feedback loop, ensuring that lessons identified are being learned and lead to continual improvement. Bottlenecks for decision-making and action and other organisational dysfunctionalities that are identified should feed into revisions of the EU Preparedness Plan and its practical implementation.

4. ARTICULATE A COHERENT VISION FOR THE EU'S ROLE IN PREPARING FOR AND RESPONDING TO EXTERNAL ARMED AGGRESSION, BY MAPPING THE FULL SCALE OF IMPLICATIONS AND LINKING DIFFERENT SECTORAL WORK STRANDS.

A shift to comprehensive preparedness can only be credible if it covers the fundamental threat of armed aggression. This needs to be embedded in the work towards a Preparedness Union Strategy as set out above. To make sure the EU is ready to act in support of an attacked Member State, we need to assess the societal, economic, security and other implications of an attack against any one Member State – and which additional measures are required, in complementarity with NATO. In this type of scenario, the EU will need to deploy its full spectrum of policies and tools, and related regulatory and financial powers. Various services of the Commission, partly together with the EEAS and the EDA, are already working with NATO counterparts on several sectoral preparedness questions related to major military contingencies.

13. In line with the 2021 amendment of Decision 1313/2013 and the EU Disaster Resilience Goals' pillar 'anticipate', the Commission, together with Member State experts, developed ten cross-sectoral, multi-country disaster and crisis scenarios with the aim of introducing a more evidence-based and forward-looking approach to disaster risk management. These ten scenarios, including, for instance, an armed conflict, a severe nuclear accident, extreme winter weather with a cyber component, or a renewed pandemic, were underpinned by 16 underlying hazards.

EU experts should therefore develop concrete scenario-based thinking to systematically assess which policies and instruments would become relevant, how to better link our respective preparedness efforts, and how to effectively coordinate their use in the final instance. NATO experts should be associated to this process. To ensure complementarity with NATO, this would also include analysing the implications of a parallel activation of either the Mutual Assistance Clause (Article 42(7) TEU) and/or the Solidarity Clause (Article 222 TFEU) – which are considered further in chapter 3. These efforts could be linked to the 'European Civil Defence Mechanism' envisaged in the Political Guidelines.

5. STRENGTHEN THE EU-NATO INTERFACE IN VIEW OF GRAVE CRISIS SITUATIONS, INCLUDING THROUGH AN EMERGENCY PROTOCOL THAT CAN BE ACTIVATED TO STREAMLINE INFORMATION EXCHANGE.

EU-NATO cooperation has accelerated significantly in recent years, notably through the broadening of the staff-to-staff dialogues and interactions on a wide range of topics of common interest in line with the three EU-NATO joint declarations. At the same time, well-known diplomatic and legal hurdles hamper the formal exchange of information and the inclusiveness of all Member States and all NATO Allies respectively. **In today's security context, renewed efforts must be made to find a way through the obstacles to seamless EU-NATO cooperation, rather than working around them.** In full respect of the agreed that govern the EU-NATO partnership, further joined-up work with NATO should be encouraged across the range of issues identified in this report:

- Scenario-based expert exchanges should help to identify civilian-military and EU-NATO intersections and potential bottlenecks in major crisis situations, including external armed aggression, from a whole-of-government perspective.

- EU-NATO coordination and information-sharing frameworks at both the political and technical level need to be further reinforced. Specifically, there is a need to overcome the lack of an agreed set of standard operating procedures between the EU and NATO for an Article 5 scenario – both at the political, and at the technical level. Given the current legal and political constraints, both organisations could agree on an emergency protocol that could be activated in or ahead of a crisis situation. This protocol could define the terms for enhanced information exchange and dialogue when it matters the most. In the event of an Article 5 scenario (including in the immediate run up to it), operational crisis management structures on both sides should be able to communicate seamlessly. The EU and NATO's leadership should also remain in close contact. Preparedness means not leaving this up to unwritten practice, but pre-emptively agreeing and exercising it.

- Coherence and mutual reinforcement between NATO's work on implementing its resilience baseline requirements and the EU's envisaged efforts to take forward its work on preparedness and readiness, building on ongoing efforts and further steps envisaged in this report. The strategic aim would be to ensure the optimal use of scarce resources and to enable both organisations to address common challenges from their respective mandates and vocations in the most effective way. Given the overlapping membership, synergies regarding inputs and reporting envisaged as part of respective processes should be actively explored, especially for Member States that are also members of NATO. This could apply, for example, to the sharing of national assessments of the implementation of the NATO resilience baseline requirements with EU actors, such as the EDA, the EEAS and Commission services.

CHAPTER · CHAPTER · CHAPTER

03

Ensuring speed of action with structures and procedures that are fit for purpose

Speed matters

Speed is essential in crisis situations. This can already be a challenge in a national setting. At the EU level, there are additional interinstitutional complexities, including regarding the availability of data and the challenge of cross-sectoral coordination. While respecting all relevant competences, there is therefore a clear need to **strengthen the EU's capacity for timely and well-informed decision-making** – both at the political and technical-operational levels – as well as for agile follow-up and implementation.

This requires **organisational clarity** and further streamlining of procedures, wherever possible. To this end, the EU and Member States need to further develop an effective and efficient division of roles and responsibilities, a **coherent and resilient coordination set-up, and reflexive information sharing** for major crisis situations.

To ensure that the EU can rise to the challenge under any circumstance, **the future Preparedness Union Strategy should propose organisational and legal changes where needed**, in line with the Treaties. This would also be in line with the pledge introduced in the new Political Guidelines (2024-2029) to stress-test the entire EU acquis with a view to its simplification and the elimination of overlaps. **The overall aim should be to further consolidate the EU's crisis management and preparedness architecture**, coalescing where possible different sectoral mechanisms and coordinating entities, and removing unnecessary institutional or bureaucratic obstacles to cross-sectoral coordination.

This requires thorough **scanning and testing of the existing frameworks, processes, and blueprints** to identify elements that need to be streamlined or strengthened, notably to ensure prepared-

ness for the most severe crisis scenarios. Beyond political level decision-making, particular emphasis should be placed on identifying **missing cross-sectoral linkages or overlaps** at the operational level to ensure rapid, effective, and cross-cutting action. In a major crisis situation, different crisis response actors will need to be able to operate seamlessly together. Moreover, robust emergency procedures and provisions should be in place internally within Commission services and the EEAS, with cross-links to the various sectoral crisis emergency provisions of relevant policy instruments[01].

This applies, in particular, to further **strengthening civil-military cooperation frameworks from planning to execution. Common, interoperable, and secure communications tools** are needed to facilitate effective operational coordination in cross-border crises, in particular, to better connect civilian and military authorities across the EU [see Box 2]

Finally, rapid action can be facilitated by **actionable anticipatory analysis and strategic foresight** to inform planning, decision-making and other aspects of preparedness. The focus should not only be on the longer term, but especially considering the geopolitical volatility of today's world, improved short-to-medium-term analysis and foresight can **enable decision-makers to shape policies and to prepare for emerging risk scenarios**. This also needs to better cover the use of intelligence analysis to support informed and timely decision-making in the EU [see chapter 6].

BOX 2

Communication in times of crisis: building new secure, resilient and interoperable systems

To respond to a major security incident or a natural disaster that requires a European response, it is essential that authorities can communicate. Today, communication equipment used by law enforcement, border guards, firefighters or medical responders cannot be used in the territory of other Member States. Moreover, in many cases, the equipment does not allow for communication between different types of responders and, in particular, with the military.

Member States and the Commission have been working on the creation of a European system that is able to connect all EU civil security and public safety authorities across borders, which could be designed to also enable interoperability with military communication systems, such as the military Communications and Information System being developed for European Union Military Staff (EUMS) / the Military Planning and Conduct Capability (MPCC). **This European Critical Communication System** (EUCCS) should be the centre of a united approach to security and preparedness, as announced in the Political Guidelines (2024-2029).

Moreover, the EU will deploy the **EU Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²)** – a secure connectivity low and medium-orbit satellite constellation that would ensure its capacity to connect crisis actors in the most demanding circumstances. IRIS² will provide resilient and uninterrupted communication and connectivity services for government and military users in the event of natural disasters, hybrid attacks, acts of aggression, or operational – civilian and military – deployments worldwide. In particular, it will contribute to the continued functioning of critical infrastructure (e.g. dams, power stations, local 5G cells), ensure the uninterrupted coordination of citizens and public authorities in the event of emergencies, and serve as backup telecommunication infrastructure for critical users in areas where terrestrial networks have been disrupted.

01. Pursuant to Articles 42(4) and 43(2) of the Treaty on European Union (TEU), civilian and military crisis management operations are established by the Council in the framework of the Common Security and Defence Policy (CSDP) of the Union. In that context, and in accordance with Article 38 TEU, the Political and Security Committee exercises, under the responsibility of the Council and of the High Representative, the political control and strategic direction of the crisis management operations.

To further enhance the security of communications, the Commission, Member States, the European Space Agency (ESA) and the European quantum industry are also working on **the development and deployment of quantum communication infrastructure (EuroQCI)**. EuroQCI will reinforce the protection of communication between Europe's governmental institutions, their data centres, hospitals, energy grids, and more by strengthening our capacity to prevent and detect potential eavesdroppers.

Data matters

Situational awareness is vital to ensuring that **decision-makers can take informed decisions in a timely manner**. Here, there is still room to improve the sharing and fusion of relevant information streams from different crisis actors within EU institutions, between them and with Member States in a timely manner. **More problematic, however, is that in critical sectors there is a lack of relevant data**. The COVID-19 pandemic demonstrated how vital it was to know the rate of infections, as well as the rate of vaccinations, to steer decisions on the handling of the pandemic. This in turn required not only new information systems, but also reliable testing methods.

Despite significant advances in terms of gathering and processing of information at the EU level, across numerous domains, **there are still deficiencies concerning the availability of data and information gaps in others. In particular in some domains that are critical for preparedness,** governmental or private sector actors remain reluctant to share relevant information, such as production rates and/or shortages, disruptions in external supply chains, the state of strategic stockpiles, available ammunition stocks, etc. Here, Member States and the private sector often cite commercial sensitivity or national security concerns – even if there could be ways to ensure confidentiality and only present aggregated data externally. **Trust and mutual understanding** among the main crisis preparedness and response actors at the EU level and across Member States should be continuously nurtured and reinforced through clear procedures, as well as regular interaction and exercising before a crisis hits. Knowing one's relevant counterparts, having established trust and practical working methods with them can buy essential time during emergencies.

Coordination matters

In major cross-sectoral and cross-border crises, multi-stakeholder coordination will be required. Moreover, we can no longer expect to deal with one crisis at a time, but need to manage and respond to various crises simultaneously. **Multiple and multidimensional crises require close coordination at the operational level, for example to effectively deliver civil protection and humanitarian assistance where needed.** The Emergency Response Coordination Centre (ERCC) plays a pivotal role in this regard [see Box 3 below]. However, as we saw in recent years, such crises can also create a situation in which a) there is a relative scarcity of certain products required to address the crisis, whether vaccines, ammunition stocks or emergency equipment; and b) an urgent need for new budgetary and economic investments to stem the financial-economic turmoil or other impacts – which can lead to competing priorities and fiscal challenges. Moreover, in the event of armed aggression, for example, **military and humanitarian/crisis actors will be asking for priority access to limited transport capacities, hospital beds, medical supplies, production capacities**, etc.

This scarcity, distribution and prioritisation dilemma is very fundamental in any major pan-European crisis. As we have seen, Member States can be tempted to close down borders, to 'hoard' these products and compete for their limited supply, with detrimental effects on the Single Market and the free movement of goods and people. In turn, however, during these past crises, we have shown

that close coordination at the EU level helped to find common solutions, in the spirit of the European project.

This goes to the heart of the most fundamental coordination challenges during a multidimensional crisis of European scale: how to coordinate – and ultimately arbitrate – the effective use and distribution of scarce resources when their demand surges exponentially. Building in buffers, resilient supply chains, stocks and redundancies is one step, but it may not be possible to be fully sufficient. **This points to the need for a strong governance mechanism at the national and EU level to ensure that efficient and well-coordinated solutions can be found.** These issues should be covered in the Preparedness Union Strategy, as laid out in chapter 2.

BOX 3

The Emergency Response Coordination Centre (ERCC)

The ERCC is a 24/7 structure within the Commission that supports a coordinated operational response to different crises by deploying civil protection and humanitarian operations worldwide. While it primarily supports the functioning of the Union Civil Protection Mechanism (UCPM), it also serves as a 24/7 point of contact for the Commission's internal crisis coordination process, Argus, and for the Council's Integrated Political Crisis Response mechanism (IPCR), supporting it with information products. The ERCC has also developed strong capabilities to anticipate emerging trends and risks, providing early warning and situational awareness. Notably, the ERCC:

- Coordinates the EU's response to climate-change induced and nature-related crises (wildfires, floods, and earthquakes) through operational deployments and the delivery of assistance under the UCPM including from **the strategic rescEU reserve**.
- Supports emergency response in complement with EU humanitarian funding (the UCPM, the Emergency Toolbox, the European Humanitarian Response Capacity), and in line with humanitarian principles.
- Plays a central role in responding to long, complex, and simultaneous cross-sectoral crises (e.g. COVID-19 and Russia's war against Ukraine), coordinating the delivery of in-kind assistance and support services, and contributing to a coherent, systematic and cross-sectoral approach.
- Coordinates with the EEAS's Crisis Response Centre (CRC) regarding the consular protection of EU citizens from third countries, with the CRC focusing on consular cooperation and coordination together with the EU Delegation, and the ERCC providing the logistical support for evacuation under the UCPM.

Strengthening the Union's capacity for ambitious and decisive action

Beyond the dimension of operational cooperation and information sharing, the EU also needs to strengthen its capacity for ambitious and rapid decision-making at the political level. Despite the understandable political sensitivity, and respecting Member States' competences, **addressing EU-level decision-making in crisis situations is of crucial importance**. In a deeply uncertain and volatile world, the EU institutions must be able to take decisions quickly. Swift action can be instrumental in stemming the unfolding crisis from escalating or cascading further. It also strengthens the credibility of the Union in the eyes of its citizens. The Integrated Political Crisis Response (IPCR) arrangements remain a key instrument in this regard.

There have been **good examples in recent years** on which we can build further. For example, the first sanctions package against Russia after its full-scale invasion of Ukraine, alongside various other actions, was announced within a matter of days. There are **also examples where Europe was struggling to keep up with rapidly unfolding events** (e.g. in the early stages of the pandemic), **proved to be politically divided** (e.g. on the situation in Gaza in the aftermath of the terrorist attacks on Israel of October 2023) or just **held up by a few or even one Member State(s) standing in the way of consensus** (e.g. in relation to the financial and military support to Ukraine).

Despite these constraints, throughout the Covid-19 pandemic and especially in response to Russia's aggression against Ukraine, the **Union has overall demonstrated that it can act rapidly and decisively when under pressure – especially when there is a shared sense of urgency**. One of the main challenges during such protracted crises is to maintain momentum to enable swift and decisive decisions even after the initial shock at the outset of the crises has evaporated. Success in overcoming severe crises is not guaranteed by the initial reaction, but is based on the ability to stay committed and resolute throughout the crisis. At the same time, it is also paramount to return to a regular decision-making pattern based on better regulation as soon as there is no more urgency to act. Measures taken during the crisis need to then be evaluated to identify lessons for our future preparedness.

Moreover, especially in the EU's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy, (CSDP) decision-making within the Council is generally based on unanimity, reflecting the sensitivity of these issues. There are also cases where the Treaties already allow for qualified majority voting (QMV) (Art. 31(2) TEU), but this possibility is often not used in practice by Member States. In crisis situations, this can **undermine the Union's ability to speak with one voice, to take rapid action, or allocate the necessary resources**.

Far from their original purpose, vetoes can be abused as bargaining chips for unrelated policy negotiations, based on national interests. In a more extreme scenario, **the veto mechanism may even be instrumentalised by foreign competitors and rivals who could exploit the dependencies and vulnerabilities of individual Member States** to interfere with and undermine EU decision-making through targeted pressure[02]. A hostile actor could use a single Member State's strategic dependencies or other forms of leverage and prevent the whole EU from taking decisions that would impose consequences on a hostile actor.

Ensuring rapid decision-making is all the more relevant in view of the EU's **future enlargement, which may increase the Union's membership to more than 30 Member States**. As such, these safeguards can pose a significant risk to the EU's readiness for decisive crisis response and its capacity for proactive preparedness, ultimately putting at stake the Union's legitimacy, credibility, and ability to deliver for citizens.

The ongoing discussions among Member States to reform the Union in view of its enlargement **should also be used to address the ways in which decision-making can be accelerated and streamlined**. The Integrated Political Crisis Response (IPCR) offers a basis to ensure flexible formats to share information and support the decision-making of the Council. In the context of the Union's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP), moreover, considerable debate has already been ongoing for some time.

Building on this, the EU and Member States should explore a package proposal of measures for enhanced EU decision-making, that could be activated when a major crisis situation erupts. This package could include:

- Shifting to qualified majority voting (QMV) in CFSP, including civilian CSDP, based on the so-called 'passerelle' clause in Article 31(3) TEU, and making full use of the already existing possibilities for QMV (Article 31(2)TEU).

- Relying on several options that allow Member States to protect their national security interests,

02. Fiott, D., & Tercovich, G., Votes, Vetoes, Values: Foreign Interference, QMV and EU Foreign Policy in a Competitive Age, CSDS Policy Brief, 2023(21), 1-4, 2023.

including through constructive abstention pursuant to Article 31(1)(2) TEU, the creation of a 'sovereignty safety net' or 'emergency brake' in line with Article 31(2)(2) TEU, and a combination of the blocking minority (Article 16(4) TEU) and the 'Ioannina compromise'.

Moreover, there is considerable potential to work together within the EU framework using special frameworks for cooperation:

- The Lisbon Treaty introduced the **enhanced cooperation instrument** under Article 20 TEU as a mechanism enabling differentiated integration within the framework of the EU treaties.
- The **Permanent Structured Cooperation** (pursuant to Article 46 TEU), in which 26 Member States participate, provides a framework for defence cooperation and concrete projects in which different groupings of 'willing and capable' Member States can join forces with different levels of ambition.

Regardless of the route taken, ensuring rapid, agile, and decisive decision-making at the political level will be an **essential catalyst for a genuine whole-of-society and whole-of-government approach** to comprehensive preparedness. This can trickle down across all levels and domains of EU action and make sure our framework is coherent and fit for purpose in view of the serious threats and hazards we must be prepared to face in the coming years.

Mutual assistance and solidarity clauses

The EU Treaties contain profound pledges of mutual support in case another Member State **falls victim of armed aggression (Art. 42.7 TEU)**, or to act jointly in a spirit of solidarity if a Member State is the object of a **terrorist attack or a natural or man-made disaster (Art. 222 TFEU)**. Paradoxically, however, preparatory work in anticipation of the possible activation of these provisions has, for different reasons, remained sub-optimal. This creates a political, strategic and operational risk in case they would be invoked during a sudden and severe crisis situation.

Fortunately, there has only once been a need to invoke the Mutual Assistance Clause (Art. 42.7 TEU), namely by France following the terrorist attacks of 13 November 2015. However, despite further deliberations on practical arrangements (including the creation of a Handbook) and various 'tabletop' exercises, **this Treaty provision still has not been sufficiently backed up by further planning, structures, or resources**. It is necessary to underline that the article itself specifies that any commitments and cooperation in this area shall be consistent with commitments under NATO, which, for those States who are members, remains the foundation of their collective defence and the forum for its implementation.

The Solidarity Clause (Art. 222 TFEU) has not been invoked even once. Its threshold for activation, as defined in the Council decision that defines its implementing arrangements[03], sets the bar rather high: namely **when national capabilities and resources are overwhelmed and exhausted**. However, the spirit of solidarity does underpin the entire Union Civil Protection Mechanism, as Member States support each other with expertise and assets in the event of large-scale natural and man-made disasters.

Without entering into an exhaustive legal analysis, **the following elements could support reflection on the way forward**:

- **The Mutual Assistance Clause (MAC) offers a powerful obligation on Member States to assist 'with all the means within their power'.** This opens up the necessary scope for whole-of-government assistance to the attacked Member State, which would be complementary to NATO.

03. 2014/415/EU: Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause.

Moreover, there might be occasions where the attacked Member State turns to the EU level for help – possibly in conjunction with an activation of Article 5 in case that Member State is also a member of NATO. Further work should be undertaken to identify the implications of such a scenario.

- The **Solidarity Clause** is restricted to terrorist attacks and natural or man-made disasters, highlighting its targeted rather than general application. However, the broader reference to natural and man-made disasters raises the question **whether the clause could also be relevant in the context of hybrid attacks, including malicious cyber operations, acts of physical sabotage, or pandemics**. Moreover, there might be a willingness to revisit the implementing arrangements agreed in 2014, in view of redefining the threshold for its activation to a crisis stage before national authorities become overwhelmed. This threshold could be changed by means of a Council Decision on the basis of a joint proposal by the Commission and the High Representative.

- Finally, there might be situations in which both provisions are activated at the same time by a Member State that is victim to armed aggression alongside man-made disasters. This will require careful coordination, given the very different institutional settings for the two provisions respectively. Article 222(1) TFEU clarifies that the **Union itself** must fulfil solidarity obligations, with specific duties defined in the following paragraphs of the provision. This ensures that the Union can provide necessary support across various disaster scenarios, reinforcing its commitment to mutual aid and cooperation among Member States.

Recommendations

1. Reinforce cross-sectoral operational coordination:

- Develop a central operational crisis 'hub' within the Commission to facilitate cross-sectoral coordination and situational awareness. This should build firmly on the existing Emergency Response Coordination Centre (ERCC), acting as a platform to connect relevant sectoral crisis management arrangements at the EU level.
- Further optimise the use of the Integrated Political Crisis Response (IPCR) arrangements in the Council to enhance coordination between Commission services, the EEAS, and Member States, and reinforce linkages between the political leadership and the technical level.
- Strengthen civil-military coordination frameworks and joint planning to ensure an effective civil-military response to a range of intentional threats – both within and beyond the EU.
- Further operationalise Articles 42.7 TEU and 222 TFEU to strengthen their credibility and operational value as expressions of a European spirit of mutual assistance and solidarity.

2. Boost and better coordinate situational awareness, anticipation, and foresight:

- Link situational analysis and intelligence assessments more closely with EU-level preparedness and decision-making processes.
- Set-up an EU Earth-Observation governmental service for enhanced situational awareness in support of the preparedness, decision-making and action of the EU and Member States in the fields of security and defence.
- Develop tools and frameworks to make our strategic foresight toolbox more actionable and solution-oriented.

3. Strengthen information sharing and communication:

- Accelerate the roll-out of secure, autonomous, and interoperable information exchange and communication systems to connect EU institutions, bodies and agencies, Member States, and key partners.
- Enhance trust-based sharing of sensitive information between willing Member States for specific purposes.
- Embed communication more closely in crisis management, including through the development of EU frameworks and modules, as well as training for local, regional, and national contact points.

4. Enhance the EU's exercise and training culture.

- Adopt an EU Exercise Policy to promote shared approaches across different sectors and institutions and bring together resources and expertise in a centrally accessible Exercise Knowledge Hub.
- Reviewing and building on existing programmes, set up regular cross-sectoral EU training courses on security, defence, and crisis management to further reinforce mutual trust and promote a common European security, safety and preparedness culture.

1. REINFORCE CROSS-SECTORAL OPERATIONAL COORDINATION

→ Develop a central operational crisis 'hub' within the Commission to facilitate cross-sectoral coordination and situational awareness. This should build firmly on the existing Emergency Response Coordination Centre (ERCC), acting as a platform to connect relevant sectoral crisis management arrangements at the EU level.

The need to strengthen lines of communication, to link up sectoral crisis arrangements and enhance civil-military cooperation calls for a step-change in ambition towards a genuinely **cross-sectoral approach to (non-CFSP) crisis management at the EU level, including in the long-run, a fully-fledged EU crisis centre**. As part of a step-by-step approach and building on the ERCC [see Box 3], the EU should develop a modular operational crisis hub. This would allow for a scaled-up and tailored response to the emerging needs of individual crisis situations, by plugging in sectoral crisis arrangements seamlessly and linking up with Member States' crisis centres. The development of such enhanced structures should fully respect the specificities of different sectorial responses, as well as the competences of the Member States and the Union in this field.

The ERCC should continue to serve routine civil protection, disaster relief, and humanitarian coordination functions. On top of this, it could be re-designed as a body that provides a single cross-sectoral entry point to be used in major cross-border and cascading crises[04]. Depending on the specificities of the crisis at hand, all relevant sectoral response actors should be able to plug in, through different 'modules' and teams, within this central hub, thus strengthening shared situational awareness, analysis, communication, and the coordination of assistance. This could apply across the Commission and should also involve strengthened links to relevant CFSP-related civilian and military structures and tools, including the EU Military Staff, the Military Planning and Conduct Capability, and the Civilian Planning and Conduct Capabilities in the EEAS. In the context of the EU's support for Ukraine or another regional or intra-EU crisis, such plug-in arrangements could be vital for the efficiency and speed of the EU's assistance measures. Different legal bases – and related decision-making procedures within the EU Institutions – have to be respected.

This approach would also ensure an **optimal use of resources and infrastructure, including robust 24/7 capabilities and secure facilities/networks.** Critically, the existing secure rooms and classified information management infrastructures available in the Commission should be upgraded and centralised whenever possible. This will be particularly important to ensure the central crisis hub's ability to manage crises with a security dimension, including in particular through the swift and secure exchange of classified information in a compartmentalised manner. Close links with relevant Commission services, the EEAS, the General Secretariat of the Council, as well as responsible national authorities of Member States should be ensured. While the central crisis hub would be responsible for horizontal coordination and first response, it would not replace critical services provided by other sectoral actors. Finally, further developing the ERCC into a horizontal crisis hub for the EU should be accompanied by further reflection on institutional and resource implications.

→ Further optimise the use of the Integrated Political Crisis Response (IPCR) arrangements in the Council to enhance coordination between the Commission, the EEAS, and Member States, and reinforce linkages between the political leadership and the technical level.

The Council should consider taking further steps to optimise the use of its IPCR arrangements with a view to enhancing coordination between the Commission, the EEAS, and Member States and reinforcing linkages between the political leadership and the technical level. For instance, this could include a further formalisation of the mandate and responsibilities of Member States' dele-

04. This would not cover consular crisis management and CSDP missions and operations, which remain under the mandate of the EEAS' Crisis Response Centre (CRC) (with logistical and operational support from the ERCC) and the EU Military Staff (EUMS)/Military Planning and Conduct Capability (MPCC).

gates and regular IPCR exercises. Another track could include further clarification of the division of labour between the IPCR and other sectoral Council working parties involved in managing a crisis. Finally, the Council could adopt a 90-day review clause to regularly assess the necessity of maintaining ongoing IPCR activations.

→ Strengthen civil-military coordination arrangements and a capacity for joint planning to ensure an effective civil-military response to a range of intentional threats.

To ensure a swift civil-military response to a range of different threats and emergencies – both within the Union and beyond, **effective coordination arrangements** between the armed forces, civil protection and emergency services, as well as other civilian (security) actors are needed. Ensuring effective civil-military cooperation at the Union level, for instance by potentially moving towards a European Civil Defence Mechanism, would also reflect and build on relevant developments in Member States. For instance, the Swedish 'total defence' concept, the establishment of a new ministry in Denmark for State security and emergency management and the recent update of civil-military cooperation frameworks as part of the new German framework guidelines for overall defence demonstrate efforts to prepare for a 'whole-of-government' response to armed aggression (RRGV)[05].

Such arrangements would need to take into account the specific status of civil defence in international law. In practice, reinforced civil-military coordination arrangements need to cover the relevant domains, including cyber, energy, intelligence, space, the economy, and critical infrastructure. Practically, **the Emergency Response Coordination Centre (ERCC) and its further evolution into a central crisis hub should further strengthen its links with the crisis management structures in the EEAS and Commission services, where relevant**. In particular, effective civil-military and security services cooperation will be crucial to **managing the consequences of hybrid attacks** on our critical infrastructure, including prolonged blackouts, disruptions of telecommunications, energy provision and water supply, disinformation campaigns, or large population displacements, as well as CBRN incidents and attacks.

→ Further strengthen the operational value of Articles 42.7 TEU and 222 TFEU as part of the EU's whole-of-government preparedness and readiness to address the full spectrum of risks.

Strengthening the operational value of these core treaty provisions during emergencies requires a careful process of considering where they can and **need to be backed up by further planning and procedural arrangements**. Building on previous efforts to strengthen procedural clarity, for instance in the context of the Mutual Assistance Clause Handbook or the Implementing Arrangements for the Solidarity Clause, the EU and Member States should **review and update such operational frameworks and guidelines**. To make sure the provisions are fit for purpose, we should, for instance, a) clarify how the envisaged assistance could be framed as part of a whole-of-government approach, b) better define and flesh out potential cases for the use of the Solidarity Clause (e.g. hybrid attacks or pandemics), c) adjust the activation thresholds of the Solidarity Clause to cover earlier stages of a crisis, and d) consider coordination mechanisms in the event of parallel activation of the two Articles.

05. Government of Sweden, Total defence, 2024.
German Federal Ministry of Defence, Federal Government strengthens Germany's military and civil defence, 2024.

2. BOOST AND BETTER COORDINATE SITUATIONAL AWARENESS, ANTICIPATION, AND FORESIGHT

→ Link situational analysis and intelligence assessments more closely with EU-level preparedness and decision-making processes.

As a first step, this would require strengthening the pooling of information gathered by different sectoral situational awareness capabilities. For instance, this task could be taken up by a future operational crisis hub [see the recommendation above]. As a second step, pooled information would need to be processed and integrated in a targeted manner to ensure an action-oriented presentation to political decision-makers. To ensure quick uptake, the EU should further streamline the transmission of relevant situational awareness and intelligence assessments from the technical to the political level, e.g. by institutionalising regular intelligence briefs with an operational focus. In addition, particular consideration should be given to further strengthening the information, data and intelligence shared by national services with the EU Single Intelligence and Analysis Capacity (SIAC), as well as reinforcing its cooperation with anticipatory analysis and contingency planning across the Commission. While SIAC provides intelligence support to Member States, the EEAS and the Commission, it does retain a particular focus on CFSP. This is why the EU should consider further reinforcing situational awareness and analysis also in non-CFSP areas [see also chapter 6].

→ Set up an EU Earth-Observation governmental service for enhanced situational awareness in support of preparedness, decision-making and the action of the EU and Member States in the fields of security and defence.

Geospatial intelligence structures, such as the EU Satellite Centre (EU SATCEN), are essential to support to autonomous decision-making and the action of the EU and Member States for security and defence. In a tense and fast-evolving geopolitical context, highly reactive capabilities are required to provide reliable satellite imagery faster and in a secured manner. There is a need to enhance space-based situational awareness towards more autonomy, accuracy and timeliness. To complement and reinforce existing and planned capabilities, the EU and Member States could develop a dedicated EU Earth-Observation governmental service.

→ Develop tools and frameworks to make EU strategic foresight more actionable and solution-oriented.

While situational awareness deals with the current situation and early warning in the short to medium term, the work on preparedness also needs to be driven reflections on mega trends and the anticipation of possible longer-term developments – in other words, strategic foresight. This process has a clear value in its won right and the EU has already produced a wide array of foresight products. However, foresight analysis also needs to be actionable, i.e. policy-makers need to be able to draw on it to explore how future developments and risks could impact their policy field in concrete ways. To this end, building on existing work strands of the Commission's Joint Research Centre (JRC), foresight products should be made more actionable and the connection between our foresight toolbox and immediate short-term policy choices should be strengthened. For instance, effective foresight products can highlight the trade-offs of mitigating different risks, and identify key actors. In addition, we should continue strengthening foresight cooperation and alliances with other EU institutions under the umbrella of the EU-wide foresight network, as well as other partners. In particular, the EU should better leverage its delegations in third countries and CSDP missions to feed information and analysis into foresight processes. This could also involve developing partnerships with foresight units in Member States or NATO, and reinforcing exchanges with like-minded partners at the regional and global level [see chapter 8].

3. STRENGTHEN INFORMATION SHARING AND COMMUNICATION

→ Accelerate the roll-out of secure, autonomous, and interoperable information exchange and communication systems to connect EU institutions, bodies and agencies, Member States authorities, and key partners.

Such information exchange and communication systems (**both terrestrial and space-based**) will be essential to ensuring the **rapid, continuous, and trust-based exchange of critical information** among key crisis responders at all governmental levels for the purposes of swift operational coordination and action. As a first step, **the EU should complete the European Critical Communication System (EUCCS) by 2030** [see Box 2 above] to securely connect all EU civil security and public safety authorities across borders. To enhance civil-military cooperation and facilitate a genuinely 'whole-of-government' response, the EU and Member States should also allow for its interoperability with systems used in the defence domain. As a second step, this should also include unified encrypted mailing, calling and videoconferencing, as well as the further **modernisation and harmonisation of the exchange of classified information**. As a complement, the ability to process sensitive and classified information in all relevant domains should be reinforced by providing secured infrastructure, as well as **encouraging – where appropriate – EU staff at all levels to apply for security clearances**. Finally, to **ensure integrated civilian and military preparedness and readiness**, deployed systems should also, where appropriate, facilitate the cross-connection of civilian security and crisis management actors with military and defence actors.

→ Enhance the trust-based sharing of sensitive information between willing Member States for specific purposes.

To **address the challenge of trust in information sharing**, which is particularly salient in some sectors, such as cyber, a possible way forward could **involve 'variable geometries'**, where groups of Member States in various configurations and, where appropriate EU institutions, are encouraged to **share information on a need-to-know basis with selected others for specific purposes**. For instance, in the case of EU-CyCLONe, the notion that sensitive information should be shared with all the network (comprising of 27 Member States plus the Commission), or not at all, is not operationally logical or expedient.

→ Embed communication more closely in horizontal and vertical crisis management, including through the development of EU frameworks and modules, as well as training for local, regional, and national contact points.

Better embedding crisis communication in horizontal and vertical crisis management, including by **increasing its timeliness and coordination**, would further **contribute to overall preparedness and societal resilience**. In particular, this would be crucial to further **minimise the impact of misinformation and disinformation**, especially Foreign Information Manipulation and Interference (FIMI). In concrete terms, this could include the **development of EU frameworks and modules, as well as training for local, regional, and national contact points**, drawing on funding at the EU, Member State and local levels. Besides strengthening coordination and rolling out shared approaches, this could enrich the governance framework of strategic crisis communication with multifaceted knowledge (scientific, technical, practical, organisational, etc.) and local experiences.

4. ENHANCE THE EU'S EXERCISE AND TRAINING CULTURE

In line with the recommendation for an EU Comprehensive Preparedness Exercise in chapter 2, the EU should further develop a comprehensive exercise culture to make sure coordination and information sharing frameworks, as well as relevant instruments, work in practice – even in the most disruptive crisis conditions. Exercising is a crucial means **of building trust among relevant crisis response actors** – including between civilian and military responders. Rather than more

exercising, this should mean **investing in smarter exercising** – both sectoral and cross-sectoral. For instance, to better serve preparedness, the link between exercising and advance planning should be strengthened. Exercise scenarios should be **based on real and credible threats and risk assessments, plans, and strategic needs**. Similarly, exercises should generally aim to better integrate **cross-sectoral and cross-border** dimensions and considerations.

→ Adopt an EU Exercise Policy to promote shared approaches across different sectors and institutions, and bring together resources and expertise in a centrally accessible Exercise Knowledge Hub

Promoting shared and comparable approaches to exercising at the EU level would ensure greater coherence and complementarity across different sectors. To this end, building on existing frameworks and guidelines, such as the CSDP Exercise Policy, the Commission guidelines, and the civil protection exercise policy, the **EU should adopt a comprehensive EU Exercise Policy that could provide a common framework, principles, and guidance to all EU institutions, bodies, and agencies**. This should also address exercise types where the Commission and the EEAS act mainly as an enabler for joint exercises between Member States. Similarly, necessary resources and expertise (e.g. on scenario-building or evaluation) could be brought together in a centrally accessible **Exercise Knowledge Hub**, also building on existing entities, such as the Civil Protection Knowledge Network, which could support services, enhance harmonisation, and provide savings and efficiency gains.

→ Set up regular cross-sectoral EU training courses on security, defence, and crisis management to further reinforce mutual trust and promote a common European security, safety and preparedness culture.

Such **courses** could fill gaps left by sectoral programmes and bring together professionals from across the EU institutions (as well as Member States), including government, military forces, politics, the private sector and civil society. Reviewing existing training offers, the aim would be to provide further opportunities to learn how the EU works at different levels on security, civil and military defence, and crisis management matters. Courses should offer participants an opportunity to share national best practices, to build shared understanding of our threat environment, reinforce mutual trust, and connect with each other. These personal connections will also contribute to enhancing practical cooperation across sectoral silos and national borders in the event of a major crisis. The European Security and Defence College, as well as similar Commission learning and development centres could play an important role in organising the courses regularly. In addition, building on the example of the Finnish National Defence courses, other Member States could envisage developing similar course offerings, bringing together public authorities, the private sector, and civil society at the national level.

CHAPTER · CHAPTER · CHAPTER

04

Empowering citizens as the backbone of societal resilience and preparedness

Comprehensive preparedness must put citizens at its core. The EU and Member States can best protect citizens by **enhancing their resilience and agency**. This means increasing citizens' risk awareness, encouraging self-reliance, and enabling citizens – in different capacities – to play an active role in ensuring crisis preparedness and first response. They are an integral part of a 'whole of society' approach that brings together not only public authorities at all levels, but also private entities, employers and trade unions, civil society organisations and individual citizens.

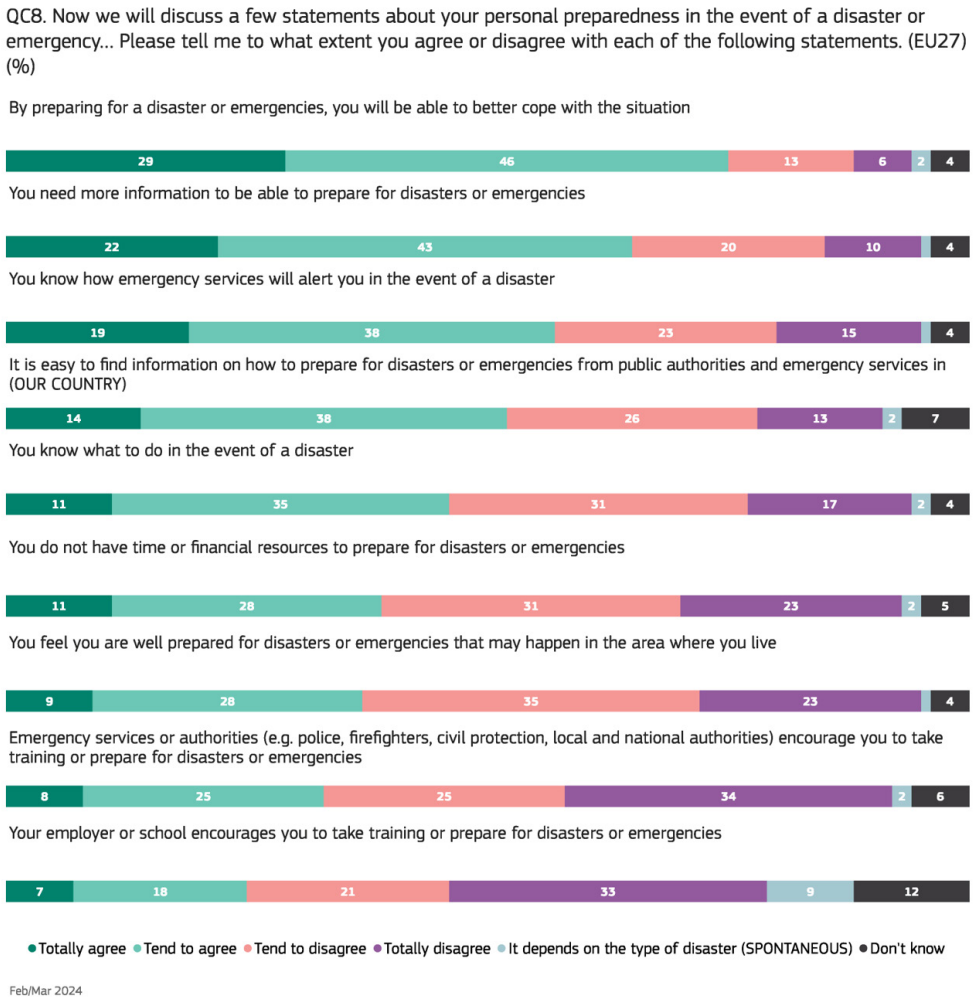
Ultimately, citizens' awareness, ability, and readiness to act to respond to a disaster or adversity are the bedrock of the EU's preparedness. This includes citizens' roles in different capacities to help protect and defend their country and therefore the EU in the event of an armed aggression. It also means encouraging their engagement in taking necessary action to tackle and prepare for the consequences of climate change and to tackle increasingly acute disaster risks.

The recent Eurobarometer survey[01] on disaster risk awareness and the preparedness of the EU population clearly showed that Europeans are increasingly aware of the multifaceted risks that may personally affect them. The survey underlined also the broad public interest in learning more about these threats, as well as ways to prepare for them. Whereas three-quarters of Europeans agree on the importance of preparedness to cope with disasters or emergencies, 65% say that they need more information to be better able to do so [see also Figure 5]. This public demand offers an important opportunity to empower Europeans to prepare better for different crises by offering them clear, useful and easily accessible information and practical concrete means to participate and contribute.

01. European Commission, Special Eurobarometer 547: Disaster risk awareness and preparedness of the EU population, 2024.

FIGURE 5

Special Eurobarometer 547 – Disaster risk awareness and preparedness of the EU population, 2024 (1)



Source: Special Eurobarometer 547, 2024.

Awareness raising

Actively engaging citizens in crisis preparedness starts with **raising their risk and threat awareness.** This applies for example to climate, health, geopolitical, and technological risks and how they can impact their daily lives. Citizens with a clear and nuanced understanding of likely risks are more capable of making risk-informed decisions and implementing individual security measures. They are also more likely to act and respond appropriately in cases of public emergency and extreme situations, such as floods, power outages, public health crises, or terrorist attacks. Ultimately, individuals and communities are the primary actors in ensuring their own safety - even before crucial first responers, such as paramedics and firefighters.

Within the Union, **different regions are exposed to climate extremes or geopolitical tensions to varying degrees**. However, in the case of pandemics or intentional threats, including armed aggression, it is important to be aware of **how interdependencies can shape overall EU security,** impacting all Member States, regions and citizens. Given the EU's highly interconnected nature, the consequences of crises can easily cascade from one sector or region to another.

Psychological resilience

Greater risk awareness needs to be accompanied by attention to citizens' **psychological resilience, mental well-being, and long-term capacity to cope** with an environment characterised by heightened risk and volatility. As seen during the COVID-19 pandemic, when the prevalence of anxiety and depression rose significantly in many EU Member States[02], protracted crises can have a detrimental impact on individual well-being and mental health, with some social groups being hit especially hard, depending on the nature of the crisis.

In addition, individual psychological resilience is critical as it enables citizens to **maintain the ability to act in their own best interests and to support the collective response to disaster or adversity, enhancing societal resilience**[03]. Particular attention needs to be devoted to protecting essential or 'frontline' workers, who underpin the EU's crisis response. For instance, during the COVID-19 pandemic, 43% of frontline healthcare workers suffered from anxiety[04]. Reinforcing transparency, communication, support services and other enablers must therefore be a key priority.

Making sure citizens are well-informed on individual preparedness measures and best practices, as well as on overall preparedness plans and crisis response measures, increases their ability to cope in the face of crisis and helps to maintain public trust in the ability of authorities to successfully manage a major crisis. Public authorities also need to show citizens that they are prepared to provide protection to them in all possible scenarios. For example, upgrading and where needed expanding civil defence shelters that can be used in the event of CRBN threats or air raids but also to provide shelter from extreme heat or for example during prolonged power cuts concretely enhances the ability to survive in a crisis, but also build trust and support psychological resilience.

In the long run, **this trust is vital to enable swift action**, to ensure public support for policy-makers and public authorities on all levels, and cooperation for necessary response or recovery measures, as well as to protect societal resilience.

Media literacy

Malicious and hostile actors use dis- and misinformation to actively to undermine the integrity and functioning of our democratic governance. Especially in a crisis situation, effective media and digital literacy will be essential to upholding fundamental tenets, such as trust in institutions, fair elections, social cohesion, and national security. The increasing fragmentation of the information landscape makes this more challenging. To further ensure we stand together during crises, we also need to **bolster citizens' ability to recognise authoritative sources of crisis response information and to dismiss disinformation and Foreign Information Manipulation and Interference (FIMI).**

For instance, as evidenced by the rise of vaccine scepticism during the COVID-19 pandemic, effective preparedness needs to take into account media literacy. Otherwise, misinformation and disinformation, as well as information manipulation, can lead to a loss of trust, polarisation and increased social divisions that are detrimental to our collective ability to cope and respond. Addressing disinformation and Foreign Information Manipulation and Interference effectively helps to foster a culture of information integrity and cognitive resilience among our citizens, and enable societies to face common challenges with unity. **It may contribute to counter the visible rise of a higher degree of distrust in government among segments of society, as part of a wider trend of polarisation and radicalisation that can also be fed by wider socio-economic concerns.**

02. European Parliament, Mental health and the pandemic, 2021.

03. Bodas, M., Peleg, K., Stolero, N., and Adini, B., Understanding Societal Resilience: Cross-Sectional Study in Eight Countries, Front Public Health, 1;10, 2022.

04. Santabárbara J., Bueno-Notivol J., Lipnicki D.M., Olaya B., Pérez-Moreno M., Gracia-García P., Idoiaga-Mondragon N., Ozamiz-Etxebarria N., Prevalence of anxiety in health care professionals during the COVID-19 pandemic: A rapid systematic review (on published articles in Medline) with meta-analysis, Prog Neuropsychopharmacol Biol Psychiatry, 20;107, 2021.

BOX 4

Education and media literacy for democratic resilience

Media literacy is crucial for navigating the news environment and making informed decisions online and offline in today's world of information overload and manipulation. Media-literate people are the first line of defence against Foreign Information Manipulation and Interference (FIMI) campaigns. They possess the necessary critical thinking skills to analyse complex realities, to assess the source of information, to be able to distinguish between facts and opinions, and detect false and misleading content. High levels of media literacy in society can also serve as a deterrence against FIMI as it makes the interference campaigns less cost-effective due to their need to be more complex and to involve more actors.

The critical nature of media literacy has been recognised in the EU's policy and action . Moreover, President von der Leyen emphasised in her Political Guidelines (2024-2029) for the next European Commission the need to focus on societal resilience and preparedness through increased digital and media literacy.

Digital and media literacy have become particularly important with the rapid development of Artificial Intelligence (AI). Coupled with its mass distribution potential using social media platforms, the **main threat of AI-generated content is not that it will make people believe things that are not real, but that it will make them question the veracity of all information, including from authoritative sources**. In this sense, AI could lead to a situation where more and more citizens are completely disengaged because the truth might seem impossible to find and where pre-disposed beliefs are further reinforced, ultimately rendering ineffective response measures in crisis situations.

Developing digital and media literacy skills and increasing the resilience of society requires the EU and Member States, together with media service providers, video-sharing and social media platforms, and civil society organisations, to support the spread of innovative tools and educational campaigns.

Some examples of innovative tools and campaigns:

- The use of '**nutrition labels**' to specify which news sources abide by certain ethical and transparency standards (e.g. see NewsGuard) could help citizens to better navigate the numerous dubious news sources appearing on their social media and/or search feed.
- Raising awareness through **gamification** is a creative way to teach people of all ages how to recognise and critically assess information. The 'Get Bad' News app, for example, allows people to step into the shoes of those disseminating fake news and to create their own disinformation campaigns. By doing so, the goal is to expose the tactics and manipulation techniques and to help people to recognise them in their daily lives. This in a way 'vaccinates' citizens against disinformation.
- **Awareness raising and media literacy campaigns by civil society organisations and EU institutions**. Many organisations are active on media literacy, but usually require support to scale up their operations. For example, Debunk.org researches disinformation and runs educational media literacy campaigns in the Baltics, Poland and Georgia. The European Commission also finances and creates supporting materials on media literacy and awareness raising (e.g. DG COMM and DG EAC developed a toolkit for teachers to start conversations with their students on how to spot disinformation). Moreover, the Commission is partnering with and is financing the **European Digital Media Observatory (EDMO)**, a network of fact-checkers, media literacy practitioners, researchers and policy experts in 28 countries across the EU and the EEA. EDMO conducted research and awareness raising campaigns for the 2024 European elections.

- **Some Member States have boosted their capacities to detect, prevent and counteract interference campaigns.** To facilitate 'pre-bunking', some Member States have been building up their institutions and have started not only to conduct media literacy campaigns, but also to proactively warn citizens when a new interference campaign is about to emerge or has been launched. For example, the French VIGINUM agency has the mandate to investigate and inform the public of manipulation campaigns (e.g. it uncovered the 'Portal Kombat' network, which is a vast system of 'information portals' disseminating pro-Russian content). Moreover, Sweden's Psychological Defence Agency cooperates with other State agencies and actors to foster societal psychological defence against Foreign Information Manipulation and Interference, working for example with the Swedish Media Council, libraries and museums to strengthen media and information literacy.

Household preparedness

Building on improved risk awareness and psychological resilience, citizens' ability to act in the face of disaster or adversity needs to be bolstered by **reinforcing individual and household preparedness and readiness** across the board. If citizens and communities across the Union are alert and ready to act and react in the event of emergency situations, they can keep themselves and others safe, offering a critical contribution to public safety. Whether facing extreme weather, a pandemic, a large-scale power outage, the impacts of a major cyberattack, or even armed aggression, citizens need to be prepared to self-sufficiently act in the first instance until assistance is mobilised or services are restored.

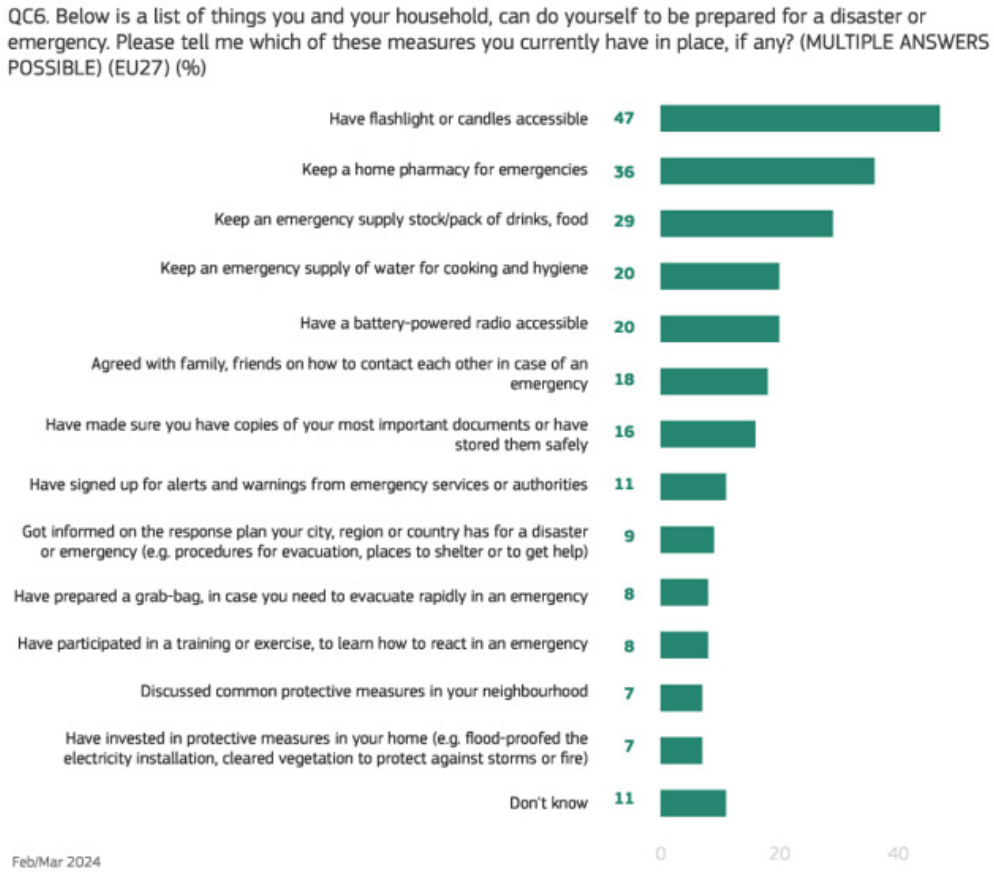
Currently, levels of household preparedness across the EU are still highly variable. In a sign of rising risk awareness, 95% of people surveyed in the EU say that their country is exposed to more than one disaster risk, with extreme weather the most frequently cited top risk. Across the EU, more than one in three citizens (37%) have personally experienced a disaster – other than COVID-19 – in the last ten years. However, **more than half of respondents do not feel well prepared for disasters (58%) and just under half would know what to do in the event of a disaster** (46%)[05]. The majority of Europeans have limited emergency preparedness measures in place [see also Figure 6], and their ability to manage basic household functions during emergencies is limited. This shows that there is **significant scope to enhance personal preparedness and household capacity to cope with disasters across the EU**, in line with the EU's Disaster Resilience Goal #2 – 'Prepare'[06].

05. European Commission, Special Eurobarometer 547: Disaster risk awareness and preparedness of the EU population, 2024.

06. European Commission, Communication on the European Union Disaster Resilience Goals: Acting together to deal with future emergencies (COM(2023) 61), 2023.

FIGURE 6

Special Eurobarometer 547 – Disaster risk awareness and preparedness of the EU population, 2024 (2)



Source: Special Eurobarometer 547, 2024.

There are already good examples from Member States on campaigns that target public risk awareness and preparedness, such as the Italian 'Io Non Rischio' (I do not risk) campaign to raise awareness on risks, including among school pupils, or the Swedish 'Om krisen eller kriget kommer' (In Case of Crisis or War) brochure and annual Preparedness Week. These examples encourage citizens' self-sufficiency in the event of an emergency and show that authorities are prepared and ready, even for the most serious threats. These good practices can be drawn upon and amplified. A more comprehensive effort could be made across the EU at all levels to educate the population on disaster risk and emergency preparedness from a young age.

The EU should strive to further raise household preparedness to ensure that every EU citizen is equipped to provide for themselves for a minimum of 72 hours in case the normal provision of basic services is disrupted in a crisis. To this end, crisis preparedness, in particular appropriate individual action in response to common risks, needs to be better integrated into education curricula, youth engagement and community outreach at the EU, Member State, and local levels. In the field of EU civil protection, the Commission has committed to support Member States to increase the overall level of risk awareness and to enhance the culture of preparedness amongst the population, as part of preparEU flagship initiative.

For EU preparedness to cover the 'whole-of-society', the EU and its Member States must further invest in household preparedness by amplifying good practices, expanding coverage to reach equally across the EU with such risk communication initiatives, and enabling this through enhanced networks of expertise. The launch of a **dedicated EU Preparedness Day** will help to reinforce a European security culture.

People with vulnerabilities and regional differences

Crises hit some people and places harder than others, often exacerbating pre-existing vulnerabilities and inequalities. For instance, the COVID-19 pandemic had a disproportionate impact on the elderly, women, low-income communities, and racial and ethnic minorities[07]. **Better protecting and engaging with people with specific vulnerabilities and bringing focus to regions at risk of being left behind should be a core dimension of building societal resilience**.

As part of a more inclusive approach to preparedness and crisis management, the EU needs to better consider the particular needs of these groups and resilience to protect social cohesion, and to maintain public trust. Public authorities need to ensure that risk assessment and risk management strategies are designed in a participative 'whole of society' approach and that particular attention is given to varied needs. For instance, representatives of groups likely to be most vulnerable to crises, such as people with disabilities, could be actively invited to participate in the design of preparedness approaches.

In addition to vulnerable groups, preparedness needs to **actively consider regional disparities that may affect societal resilience and cohesion, and ultimately undermine the EU's ability to cope in a serious and protracted crisis**. For instance, the pandemic accelerated depopulation trends and demographic shifts in certain regions. Preparedness measures should therefore take into account regions at risk of falling into the talent development trap and how this may affect their crisis resilience. This includes in terms of access to disaster response capabilities and infrastructure, such as health-care and emergency response services. Urban and rural environments present very different crisis preparedness challenges.

BOX 5

Urban resilience - Smart Cities initiative

Urban environments, with their high population densities and complex systems, are particularly vulnerable to a range of threats, from cyberattacks to natural disasters. **Urban resilience has become a critical focus** for cities worldwide. Smart city technologies play a pivotal role in enhancing it by leveraging data, connectivity, and innovative solutions.

One key aspect of this resilience is **the integration of advanced sensors and Internet of Things devices throughout urban infrastructure**, to provide real-time monitoring and data collection that proves valuable for early warning (e.g. weather patterns) and rapid response, or for the better management of critical infrastructure, such as energy grids, water supply, transportation systems, and the structural integrity of buildings. Technologies, such as green roofs, smart water management systems, and energy-efficient buildings, help cities to adapt to climate change and to mitigate the impact of extreme weather events. By analysing this data, city planners and emergency services can make informed decisions to mitigate risks, allocate resources efficiently, and coordinate responses to emergencies more effectively.

Smart cities are enhancing urban resilience through the use of advanced communication systems that ensure the rapid dissemination of information to citizens and emergency responders during a crisis (including by using mobile applications and social media). This helps to keep the public informed and engaged, to provide updates, safety instructions, and recovery information in real-time. Connectivity not only helps in managing the immediate impacts of disasters, but also fosters a sense of community resilience by keeping citizens informed and involved in the response efforts. It is essential to the success of urban resilience initiatives.

07. Liu, E., Dean, C.A., Elder, K.T., Editorial: The impact of COVID-19 on vulnerable populations, Frontiers, vol. 11, 2023.

Smart city technologies **empower residents to participate actively**. Using these tools, they can report hazards, participate in disaster drills, and volunteer for emergency response roles. Moreover, educational programmes and digital tools are used to raise awareness about resilience practices and to encourage proactive behaviours. The synergy between advanced technologies and an active and participative citizenry forms the backbone of urban resilience, ensuring that cities can not only survive, but thrive in the face of adversity.

By leveraging smart city technologies, the EU can help urban areas to become more resilient and capable of withstanding and quickly recovering from a variety of threats. This focus on resilience not only enhances immediate response capabilities, but also contributes to long-term adaptability and sustainability, which are essential for the prosperity and well-being of EU communities. The EU is funding projects in various sectors and regions to provide sustainable and innovative solutions to help communities and cities to become more resilient to current and future challenges.

Tackling skills gaps and supporting active citizenship

Closing the EU's skills gaps and tackling personnel shortages in sectors critical for preparedness should be another clear priority in terms of 'whole of society' preparedness. Member States' armed forces, civil protection and emergency services, law enforcement, as well as professional domains key to resilience, including cybersecurity, are confronted with growing recruitment challenges or shortfalls. This also applies to the private sector, including the defence and aerospace industry, and critical infrastructure operators. The lack of sufficient professionals with highly sophisticated technical skills is of particular concern. For instance, according to a recent Eurobarometer, over half of the companies searching for cybersecurity professionals face difficulties, primarily due to a lack of qualified candidates (45%), general candidate shortages (44%), lack of awareness (22%), and budget constraints (16%)[08].

In a major crisis, such as another pandemic, but especially also in a context of armed aggression, a lack of skilled workforce due to mobilisation, conscription, or free movement restrictions would pose a significant challenge to the EU's industrial, economic and societal resilience. A large-scale mobilisation of skilled workers for military operations could lead to disruptions in other critical sectors. Better preparedness therefore also means deliberately widening the labour force in critical sectors, including by reskilling and up-skilling citizens, trained volunteers, and by putting in place mechanisms to ensure the sufficient availability of skilled labour in the most critical sectors. As a long-term measure, the EU and Member States should also develop specific incentives to increase the appeal of defence, security, and emergency response-related careers. Recent opinion polls from some Member States show growing public support for the reintroduction of national service or conscription[09].

Moreover, **civil protection and emergency services in many EU Member States draw routinely upon volunteers**. Immediate first response to many disasters is through local community-based action. To address existing shortfalls and to continue to engage citizens in active volunteering from a young age, volunteer organisations also require resources, with support from the EU on risk awareness and training opportunities.

08. Flash Eurobarometer 547, Cyberskills, 2024.

09. For instance, in France, 66% of respondents regret the abolition of compulsory military service. In Belgium, 43% are in favour of the reintroduction of conscription. In Germany, 77% of respondents and majorities in all party supporter groups are in favour of young people having to serve either a year in the armed forces or in the social sector. In Lithuania, 63% of respondents support the idea of introducing mandatory military service for all persons after they graduate from secondary school. In the Netherlands, six out of ten respondents support the introduction of a new active conscription plan with young people aged between 18 and 25 having to choose between a year in the army or a year of social service (e.g. in the healthcare sector). **Note: The share of respondents favourable among younger age groups that would actually be affected by such measures drops significantly in most countries.**

Recommendations

1. **Enhance individual and household preparedness:**

- Jointly invest in citizens' risk education, incorporating different dimensions, such as cyber-security, disaster risks and disinformation.
- Promote a target of 72-hour self-sufficiency through coordinated information campaigns.
- Involve civil society organisations, as well as trade unions and employers, to enhance preparedness in different walks of life.

2. **Reinforce crisis and emergency communications with citizens by improving alert mechanisms and early warning systems to ensure a capacity to reach citizens under all conditions.**

3. **Prepare to better tackle vulnerability to crises and disasters:**

- Further invest in disaster risk management for people that are disproportionately affected by disasters and other crisis situations, and ensure inclusive disaster preparedness, also at the community level.
- Prepare in advance to minimise the disruption of protracted crises on social cohesion and the socio-economic fabric of our societies.

4. **Address skills gaps and the risk of labour shortages during crises, and promote active citizenship:**

- Implement forward-looking measures, such as mapping workforce needs, training new segments of the labour force, facilitating the inflow of skilled workers, or putting in place mechanisms for labour mobility during crises.
- Develop targeted incentives to increase the appeal of careers in defence, security and emergency response among younger generations, working also together with trade unions and employers' organisations.
- Reinforce channels and opportunities enabling the active participation of young people in preparedness action by stepping up support to the voluntary sector.

1. ENHANCE INDIVIDUAL AND HOUSEHOLD PREPAREDNESS:

→ Jointly invest in citizens' risk education, incorporating different dimensions, such as cybersecurity, disaster risks and disinformation:

Under its flagship campaign for disaster risks, 'PreparEU', the EU has already taken an important step in the direction of coordinated risk awareness action. Citizen outreach and educational campaigns should:

- **Be tailored to local contexts**, while also addressing general EU core messages on overall risks and threats.
- **Reassure and enable citizens**, by not only raising risk awareness, but also emphasising ways in which citizens can cope with threats and hazards. This includes sharing simple best practices that can be implemented at the individual level, e.g. for cybersecurity, first aid, self-defence, media and digital literacy, and 'do's and dont's' during public emergencies. Solution-oriented awareness raising campaigns stressing positive agency are much more likely to induce behavioural change without stoking further fear and anxiety[10].
- **Reach all parts of society**, including young people, the elderly, those with mobility or sensory restrictions or learning disabilities, ethnic and racial minorities, and people unfamiliar with local languages and conditions.
- **Use a range of context-appropriate communication means** that can reach all target audiences.

Targeted exchanges among Member States could help to identify, update and disseminate easily transferable best practices. The gradual integration of crisis preparedness and risk awareness, as well as media and digital literacy, into education programmes and curricula across the EU could be an additional option to ensure structural investment in societal resilience.

→ Promote a target of 72-hour self-sufficiency through coordinated information campaigns.

Individual and household preparedness should also be enhanced through coordinated information campaigns. Building upon the EU's Disaster Resilience Goal 'Prepare' and its recommended flagship campaign 'PreparEU', the EU should aim to ensure households throughout the EU are **prepared for minimum 72-hour basic self-sufficiency** regardless of the emergency (e.g. by providing common or coordinated guidelines on stockpiling, evacuations, CBRN situations, access to medical services or schooling in emergencies, etc.). Recommended preparedness measures should be locally tailored and take into account national differences relating to demographics, climate, or exposure to specific security threats. The EU could also establish a common repository of guidelines to ensure citizens can easily access context-appropriate and up-to-date guidance across the Union in a multilingual format.

10. For instance, the Commission's Joint Research Centre (JRC) has studied the behavioural change of individuals in face of cyber threats. In this context, two meta-analyses of the Protection Motivation Theory (PMT) literature, largely taken from academic studies in the health domain, have shown that campaigns that emphasise ways in which citizens can cope with threats, rather than simply raising awareness of the threat itself, are much more likely to lead to behaviour change, and should not increase fear or anxiety.
See: van Bavel, R., Rodríguez-Priego, N., Vila, J., and Briggs, P., Using protection motivation theory in the design of nudges to improve online security behaviour, International Journal of Human-Computer Studies, 123, 2018, pp. 29-39.
See: European Commission, Nudging Online Security Behaviour with Warning Messages: Results from an online experiment, 2016.

→ **Involve civil society organisations, as well as trade unions and employers, to enhance preparedness across different walks of life.**

As the recent Eurobarometer on citizens' disaster risk awareness shows, the majority of Europeans are aware of the increasing risks that may affect their own livelihoods and express a growing need for more information to enhance their personal preparedness. To make sure preparedness-relevant information can effectively reach all citizens – regardless of their position in society – the EU and Member States need to take advantage of all available platforms and means to reach different audiences. In the spirit of a genuine whole-of-society approach, the EU and Member States should therefore further engage civil society organisations, as well as trade unions and employers' organisations in this regard. Civil society organisations and social partners' should be encouraged to use their networks to help people access verified and trusted information on preparedness from the organisations' fields of expertise, as well as to learn necessary skills to improve their own level of preparedness in different contexts, including in workplaces. Trade unions and employers also have an important role in addressing the skills gap in security-related professions [see recommendation 4 below].

2. REINFORCE CRISIS AND EMERGENCY COMMUNICATION WITH CITIZENS BY IMPROVING ALERT MECHANISMS AND EARLY WARNING SYSTEMS TO ENSURE A CAPACITY TO REACH CITIZENS UNDER ALL CONDITIONS

In addition to improving citizens' structural risk awareness, the EU and Member States need to further reflect on how to **improve their ability to reach citizens under all conditions to provide early warnings, or to inform them of imminent risks and protection measures**. According to a recent Flash Eurobarometer, 79% of EU citizens agreed that, in addition to communication by national authorities, the EU should play a more active role in providing timely information and guidance to citizens in a major crisis[11]. Apart from various national measures, the Galileo Emergency Warning Satellite Service – currently under development – will be capable of sending alerts to 2.5 billion Galileo enabled smartphones (and to any other Galileo enabled devices, such as cars). While integration into national alert systems would be up to Member States to consider, its use by the EU should also be explored.

Member States' crisis communication or alert apps and other backup early warning systems should regularly be tested and surveyed for gaps and for interoperability. Lessons learned on the use of these systems [see also Box 6] during the COVID-19 pandemic in Member States and other major recent disasters, notably sudden onset extreme weather events should be analysed to guide further efforts. Additionally, the ongoing experience of the Ukrainian authorities in finding solutions to ensure communication to citizens during the Russian war of aggression should be examined for specific preparedness lessons in the context of war. For instance, Ukraine's Diia app (Дія, meaning 'action', or the acronym for Держава і Я, meaning 'State and me') was initially created to provide digital government services, but then adapted to send alerts during the Russian invasion. It provides citizens with real-time information about threats and safety measures, such as air raid warnings, and has been crucial in helping citizens to stay informed and take shelter during attacks. Given the increasingly important role of social media for information sharing in crises, particular emphasis should be placed on improving public-private cooperation in this regard, for instance through further structured dialogues with digital service providers.

11. European Commission. Flash Eurobarometer 546 – Perceptions of EU crisis management. 2024.

BOX 6

Best practices on citizen alert and crisis communication digital systems and apps

Effective citizen alert and crisis communication systems are critical for ensuring public safety during emergencies. These systems are designed to quickly disseminate information to the public to help them to make informed decisions, and to take appropriate actions in response to various threats and hazards.

Experience shows that the most successful alert and crisis communication systems for citizens include the following characteristics:

- **Multi-channel distribution:** utilise a variety of communication channels (SMS, email, social media, mobile apps, television, radio, and sirens) to reach as many people as possible, to ensure redundancy and reduce the risk of a single point of failure.
- **Geo-targeting:** functionality that allows sending alerts to citizens based on their location allows for more relevant and localised messaging, ensuring that alerts are pertinent to those in the affected area, and reduce unnecessary alarm.
- **Clarity and brevity:** messages are clear, concise, and actionable; these provide specific instructions on what actions to take (e.g. evacuate, seek shelter). and avoid using technical jargon or vague language that may cause confusion.
- **Accessibility:** ensure that alerts are accessible to people with disabilities and those who might not speak the local language. This includes by using text-to-speech technology, sign language interpreters, and multilingual support.
- **Regular testing and updates:** regularly test systems to familiarise the public with the alert system, and to ensure they are functioning correctly. Make improvements based on feedback and technological advancements.
- **Public education:** educate the public about the alert system and what to do when they receive an alert. This can be done using public service announcements, school programmes, and through community outreach.

At the global level, the most famous examples of such digital systems and apps that could inspire a European one include Ukraine's 'Diia' app [see above], Belgium's 'BE-Alert', the US' 'Emergency Alert System' and 'Wireless Emergency Alerts', the Australian 'Warning System', and Japan's 'J-Alert'.

At the EU level, the adoption of the European Electronic Communication Code Directive set a best practice by obliging Member States to ensure by 21 June 2022 that public warnings are transmitted through mobile operators or other means equivalent in terms of coverage and capacity to reach end-users. So far, most EU Member States have implemented cell broadcast or location-based SMS systems. Few Member States implemented an application that is not equivalent with cell broadcast or location-based SMS in terms of effectiveness.

The Galileo Emergency Warning Satellite Service (EWSS), which is under development by the European Commission will further complement EU Member States' Public Warning System with a satellite network to transmit warning messages to citizens. Galileo EWSS will provide a catalogue of messages in 24 languages. It will be soon available to Member States for testing and embedding in their national system.

With these initiatives, combined with EU-mapping, detection and warning services, such as the Copernicus Emergency Management Service, the EU is already setting an example for other regions under the Union Disaster Resilience Goals, and contributes to the UN Early Warning 4 All initiative.

However, additional improvements are required to ensure early warning for all, regardless of regional economic disparities (also in areas where local authorities lack the resources to develop their own systems). In an emergency, access to information is a critical tool that can make the difference between safety and harm.

The extension of the Galileo EWSS application to a Europe-wide alert app could bring significant benefits to the EU, its Member States, and citizens.

A **Europe-wide citizen alert app** would not only strengthen individual and collective resilience to crises, but also embody the principles of solidarity and cooperation that are central to the European project, ensuring the safety and well-being of all who live in or visit the EU.

3. PREPARE TO BETTER TACKLE VULNERABILITY TO CRISES AND DISASTERS:

→ **Further invest in disaster risk management for people who are disproportionately affected by disasters and other crisis situations, and ensure inclusive disaster-preparedness at community level.**

The EU and public authorities at all levels need to pay extra attention to reducing the vulnerability to disasters of certain groups, such as the elderly, people with disabilities, people with chronic diseases, or pregnant women. Ideally, people with vulnerabilities should be actively involved in preparedness by design. In particular, the elderly are disproportionately represented among fatalities and cases of ill health caused by disasters[12]. The EU already invests considerably in reducing vulnerability to disasters. For instance, under the current Multiannual Financial Framework (MFF), 14 billion euros in Cohesion Funds have already been allocated to disaster risk management and civil protection, for instance with the expectation of reducing the vulnerability of more than 40 million people to flood risks, and of more than 130 million people to wildfire risks. However, further reflection is needed on how to provide targeted support to individuals that are disproportionately affected, also placing greater emphasis on threats and risks beyond natural-hazard-induced disasters.

In this regard, we also need to reflect further on possible lessons from partners, such as Japan, which have considerable experience with addressing vulnerability to sudden onset disasters. Beyond making sure that information materials and campaigns specifically target people with particular vulnerabilities [see the recommendation above], this could include reflecting on the need to establish contact lists of individuals at the county or city-level that are particularly vulnerable to disasters and which may require evacuation support or other assistance in certain scenarios. On the basis of such lists, in Japan, some cities and counties develop evacuation plans for retirement homes or hospitals and sometimes even for individual citizens. Dedicated training and exercising of these evacuation plans contributes to overall readiness and specifically to the protection of vulnerable groups[13]. To enhance readiness at the local level, associations of local volunteers and social workers could also be supported nationally and through EU crisis preparedness programmes and networks.

12. Prohaska, T.R., and Peters, K.E., Impact of Natural Disasters on Health Outcomes and Cancer Among Older Adults, The Gerontologist, volume 59, 2019.

13. Heimberger, J-F., Évolution des mesures de réduction de la vulnérabilité des personnes aux catastrophes naturelles au Japon. Quel enseignement pour la Corée du Sud ?, Fondation pour la Recherche Stratégique, 2023.

→ **Prepare in advance to minimise the disruption of protracted crises on social cohesion and the socio-economic fabric of our societies.**

As we experienced during the COVID-19 pandemic, protracted crises can have a highly uneven socio-economic impact, further entrenching inequalities and regional disparities. For instance, during the early pandemic, spikes in unemployment disproportionately affected workers born outside of the EU, those with a low level of education and young persons. Similarly, there was considerable regional variation in terms of the impact on GDP of COVID-19 shocks[14]. While the EU and Member States quickly stepped into action, for instance through SURE – the EU's programme to finance short-term employment schemes across the EU – we can do more to prepare in advance to cushion the negative socio-economic impacts of protracted crises. Concrete proposals to bolster the crisis preparedness of vulnerable groups and regions at risk of being left behind could be further developed as part of the upcoming EU Anti-Poverty Strategy announced in the new Political Guidelines (2024-2029).

4. ADDRESS SKILLS GAP IN CRITICAL SECTORS AND THE RISK OF LABOUR SHORTAGES DURING CRISES.

→ **Implement forward-looking measures, such as mapping workforce needs, training new segments of the labour force, facilitating the inflow of skilled workers, or putting in place mechanisms for labour mobility during crises.**

With its Internal Market Emergency and Resilience Act (IMERA), the EU already has a concrete tool at its disposal, enabling it to trigger an Internal Market emergency mode that can facilitate the free movement of workers and service providers from other Member States to where they are needed. However, further steps may be needed to **address skills gaps and the risk of shortages in sectors critical to crisis preparedness**. To this end, crisis preparedness should become an important dimension of the Skills Union pledged in the Political Guidelines (2024-2029) for the next mandate. The EU could take various measures, including a **mapping of the relevant workforce and skills needs**, promoting the training of new segments of the labour force, facilitating the inflow of skilled workers/professionals, or putting in place mechanisms supporting labour mobility during crises. Concrete options could include:

- **Mapping the workforce availability and gaps in relation to EU crisis preparedness**. Among others, this should include militaries, emergency response services, law enforcement, health services, as well as other relevant sectors.
- **Adapting the modus operandi of the current Pact for Skills and Skills Academies** (the Net-Zero Industry Act, the Critical Raw Materials Act, the Batteries Academies) to a crisis management context to reskill, as appropriate, previously inactive parts of the population, available to join the workforce. However, this would require further fine-tuning, as current tools are being developed for specific categories of skills that may not be the most crisis-relevant. Further action may also be needed in the context of the EU Cybersecurity Skills Academy, including through increased EU funding and possible certification/attestation mechanisms.
- **Further speeding up the cross-border recognition of professional qualifications**, in particular in crises situations, as a means to facilitate the mobility of professionals inter alia towards regions most affected by labour shortages.
- **Putting in place more efficient procedures for the posting of workers**, for example via an EU-level 'e-declaration', that could facilitate the swift dispatching or deployment of maintenance staff/engineers for critical infrastructure in the event of a crisis.

14. European Commission, Employment and Social Developments in Europe 2021, 2021.
Eurofound, Economic and social inequalities in Europe in the aftermath of the COVID-19 pandemic, 2023.

→ Develop targeted incentives to increase the appeal of careers in defence, security and emergency response among younger generations.

To further address recruitment challenges, the EU and Member States should identify targeted incentives, including through EU-funded programmes, to make professional careers and education programmes relevant to security and emergency response more familiar and appealing to younger generations. Trade unions and employers' organisations across the EU should also be engaged in considering these incentives. Possible actions could be introduced as part of the Quality Jobs Roadmap announced in the Political Guidelines for the next mandate. Ensuring positive recognition on the labour market for State service performed could serve as an initial goal. In addition, structured exchanges among Member States could help to identify best practices in relation to **national service and conscription models, education programmes, the build-up of functioning reserve systems**, etc. that can serve as inspiration to others, are potentially transferable, and can be further facilitated at the EU level. Member States should be encouraged to explore the development and scaling-up of proven best practices. One example is the Estonian model of 'cyber conscription', which allows young people to become cybersecurity experts during their civil or military service. EU efforts should build on and complement ongoing discussions and initiatives on national service and conscription models unfolding across different Member States, such as Poland, which recently developed a voluntary one-year basic military service, or Germany and the Netherlands, which are considering a Swedish-style model of selective compulsory service[15].

→ Reinforce channels and opportunities for the active participation of young people in preparedness action by stepping up support to the voluntary sector.

As highlighted above, immediate first response to many disasters draws heavily on local community-based action and volunteering. To address existing shortfalls in the voluntary sector and to continue to engage citizens in active volunteering from a young age, volunteer organisations also require resources. In particular, there is an opportunity to link young people's concerns about the impact of climate change with positive action for broader societal resilience. To this end, the EU should explore additional opportunities to volunteer for crisis preparedness through existing EU-programmes, such as the European Solidarity Corps, and step up dedicated engagement with established youth movements on crisis preparedness – for instance, in the context of the upcoming Youth Advisory Board announced in the Political Guidelines (2024-2029).

15. Carnegie Endowment for International Peace, Europe's Conscription Challenge: Lessons From Nordic and Baltic States, 2024.

CHAPTER · CHAPTER · CHAPTER

05

Leveraging the full potential of public-private cooperation

Private businesses and the public sector as preparedness partners

Past crises have clearly demonstrated that the private sector's preparedness and resilience is vital to ensuring the continuity of vital governmental and societal functions. Private businesses, as well as public enterprises including State-owned companies, provide essential goods and services. These include energy, transport, food, water supply and wastewater disposal, and medical supplies that are critical, including in times of crisis. Many of the private companies involved are multinational and operate across the Single Market. Moreover, companies and providers operating across different sectors are interlinked. **These interdependencies between different sectors and across borders create the potential for severe knock-on effects in crisis situations, as we have seen in recent years.**

The EU's economy is also intertwined with the global economy. Research indicates that the more than 300 million companies around the world are connected through an estimated 13 billion supply and demand links, establishing relationships between buyers and suppliers for goods and services[01]. As the world's largest trading bloc and a significant regulatory power, the EU is a key interlocutor driving the global economic network and regulatory change with its 31 million enterprises, of which 99.8% are small and medium-sized enterprises (SMEs)[02]. At the same time, the EU's share of the global economy has been shrinking since the 1990s with most global growth created outside of Europe, given technological catch-up of third countries. The report of Special Adviser Mario Draghi on the EU's competitiveness makes relevant proposals for further consideration on ways to reverse this trend.

01. Pichler et al., Building an alliance to map global supply networks, 2023.

02. European Commission, Key figures on European businesses, 2024.

The EU is relatively more dependent on global trade than the US or China. In 2023, the trade-to-GDP ratio of the EU increased to 22.4%, while China's has been dropping to 18.6% and the US' to 12.7%. Even if China's share of global trade has expanded, its domestic market has grown even faster[03]. The EU's significant dependence on imports of fossil energy and near-total dependence on imported refined minerals are much higher than for the United States and China. These dependencies, as well as their concentration on a limited number of suppliers, weakens the EU's resilience and ability to respond effectively in crises, making risk mitigation essential. In 2022, the EU imported 97.6% of its natural gas, 97.7% of its oil, and 100% of its uranium. As demand continues to grow, the EU remains heavily reliant on external sources for critical raw materials vital to its industries, often depending on a single country. China supplies 100% of the EU's heavy rare earth elements and 97% of its magnesium, while Turkey provides 98% of its boron, and Brazil 92% of its niobium[04].

From a preparedness perspective, the recent succession of crises and disruptions has exposed various vulnerabilities of the EU's supply chains. This has led to delays, price fluctuations, disruptions, and shortages for consumers. Russia's war of aggression against Ukraine has revealed the strategic cost of the EU's dependence on cheap energy imports from Russia, but at the same time it has showed that Member States who took decisive action without delay have been more successful in ridding themselves of this dependence than many experts initially predicted. De-risking Europe's external dependencies and global supply chains, which have expanded over the past decades, has come to the fore in light of the growing risk of disruptions and their potential weaponisation. The 'just-in-time' principle that has lied at the heart of supply chain management to maximise cost-effectiveness in an increasingly globalised economy is now being balanced with the need for greater shock-absorption, diversification and 'home-shoring' or 're-shoring'. Private companies, as well as the EU in the context of its open strategic autonomy (OSA), are seeking the right balance between acceptable levels of cost and risk.

Reconciling Europe's competitiveness and economic growth, while managing new vulnerabilities and demands in light of the securitisation of our economies requires a major transformation. Added to these challenges are the accelerating pace and scope of global strategic competition over resources and technologies. The Economic Security Strategy (June 2023) has opened a new chapter for the EU in this regard, focusing on the resilience of supply chains, the physical and cybersecurity of critical infrastructure, technology security and technology leakage, as well as risks of the weaponisation of economic dependencies and economic coercion[05]. As external circumstances continue to deteriorate and several countries continue to anticipate and adapt to EU policies with more aggressive de-risking measures, the EU needs to further integrate economic security across policy domains and actions, in close cooperation in particular with our G7 partners.

In light of these trend lines, there is growing convergence between the interests of the government/public policy and those of the private sector from a preparedness perspective. Prosperity and security are more closely intertwined as geopolitical crises, disruptions and shocks could have profound ramifications across different economic sectors, and societies at large. **Reinforcing public-private cooperation is necessary to help minimise the risks arising from certain foreign direct investments and increased geopolitical tensions, and to better protect European companies from becoming targets of economic coercion**[06]. Moreover, measures such as inbound (and outbound) investment screening, export controls on dual-use items, risk assessments for critical technologies and supply chains, and international procurement and foreign subsidies regulations will help to integrate economic security objectives more effectively into broader European policies.

03. Eurostat, World trade in goods and services - an overview, 2024.

04. European Council, An EU critical raw materials act for the future of EU supply chains, 2024.
Eurostat, Energy statistics – an overview, 2024.

05. European Commission and High Representative, European Economic Security Strategy (JOIN(2023) 20 final), 2023.

06. Norton Rose Fulbright, EU Anti-Coercion Instrument: Key takeaways for businesses, 2024.

Closing the gaps in the EU's resilience ecosystem

The EU needs to further strengthen its support promoting the resilience and preparedness of the private sector. Efforts to bolster the regulatory framework cut across different policy domains, including critical infrastructure, economic security, competitiveness, the green transition, defence industrial readiness, as well as countering hybrid threats and other malicious activities. In particular, the 2022 adoption of the Critical Entities Resilience (CER) Directive and the Network and Information Security 2 (NIS2) Directive has established a new, comprehensive framework for the physical and cyber resilience of critical entities, expanding the sectoral scope, obligations for Member States and entities, as well as reinforcing cooperation frameworks at the EU level. The directives provide an opportunity to restructure public-private cooperation in the resilience domain, while also leading to a harmonisation of rules between Member States. **Considering that the deadline for transposition recently passed and given the crucial role of critical infrastructure for preparedness for major crises, it is indispensable that Member States ensure the implementation of those laws without delay**.

Additional sectoral and cross-sectoral initiatives further complement this resilience-building regulatory effort. Among others, this includes the Internal Market Emergency and Resilience Act, the Critical Raw Materials Act, the Net-Zero Industry Act, the Digital Operational Resilience Act, the Cyber Solidarity Act, the Cyber Resilience Act, as well as the European Food Security Crisis preparedness and response Mechanism (EFSCM).

The full implementation of this legal framework will serve as a crucial step towards a genuine, comprehensive culture of public-private cooperation for comprehensive preparedness. Recent examples, such as the successful 2023 resilience stress test in the energy sector, highlighted the significant potential of cooperation between operators and Member State authorities based on an EU-wide approach. Nevertheless, the EU has to do more to enhance cooperation, to level up the preparedness and readiness of private and public sector businesses, and to improve its capacity for a coordinated and swift response across all involved parties.

Stakeholder dialogues have shown that private and public sector companies in critical sectors, including energy, food, water, pharmaceuticals, chemicals, digital, defence, and others are keen to explore improved cooperation with public authorities. Several challenges are still hampering the effectiveness of public-private cooperation and slowing down efforts to close gaps in the EU's resilience ecosystem. Notably, these include:

- **Insufficient coordination and communication between public authorities and private entities**: In particular, lacking channels for the timely, secure, and mutual exchange of information hinder effective crisis response and preparedness action. This includes the exchange of sensitive information, for instance the sharing of intelligence and early warnings by intelligence services and other public authorities, as well as the sharing of information on vulnerabilities, stocks, and production rates by private operators. An insufficient capacity to share information at the EU level in a secure and trusted manner undermines the ability of both public and private entities for **effective risk management**.

- **A rigid regulatory environment and a lack of consistent emergency provisions**: A lack of targeted flexibility provisions and crisis-relevant derogations in legislation can undermine the speed and coherence of public-private crisis response measures.

- **Insufficient integration of resilience planning and inconsistent preparedness standards:** The integration of resilience and preparedness into businesses' core corporate strategies remains patchy. This can lead to inconsistent and inadequate crisis management practices. In addition, there is a lack of standardised training and awareness raising programmes, leading to varying levels of preparedness and response capabilities across sectors. A lack of sustained cross-sector coordination and dialogue on resilience compounds this challenge of uneven preparedness.

- **Incomplete sectoral scope of the EU-level resilience framework**: The current CER and NIS2 directives leave out certain sectors that are important for preparedness, including in the event of possible armed aggression against an EU Member State. Europe's defence industrial and technological base, for example, falls in principle outside their scope. Moreover, there are other industries and economic operators – beyond those that are already covered under the two directives – that play a crucial role in providing essential services in times of crisis, for which more stringent preparedness baselines are required, or for which the application of cybersecurity requirements should no longer only be optional. For instance, this includes key manufacturing. These omissions may result in an uneven level of preparedness and leave certain vital sectors – and hence society as a whole – vulnerable in times of disruption. Member States have the possibility to integrate these elements on a voluntary basis, but a European approach would be more effective.

- **Inconsistent or insufficient strategic stocks and supply chains vulnerable to disruption**: Businesses have long-established global structures and value chains which can restrict the ability to monitor and respond in crisis situations, and as a result prevent rapid response. In addition, both public and private actors are confronted with insufficient and inconsistent strategic stockpiles of inputs vital in crisis situations, including energy, critical raw materials, and other goods. There is also a lack of 'ever-warm' facilities to make the increased domestic production of critical goods possible within the Single Market in the event of shortages and disruptions to external supply chains.

- **Complex public procurement rules that do not sufficiently consider preparedness-by-design**: Depending on their design, public procurement rules can have a significant impact on preparedness, for instance by strengthening the resilience and protection of critical sectors. Further steps are needed to ensure EU rules contribute to the continuity of the EU's critical functions under all circumstances.

An EU-wide strategic stockpiling regime

The question of strategic stockpiling deserves special attention in terms of public-private cooperation for crisis preparedness. A comprehensive push to strengthen public and private reserves of strategic goods and materials would mitigate the impact of sudden supply chain disruptions and price fluctuations with the potential to affect the functioning of States, societies, and businesses. It would provide a higher level of preparedness and readiness to face possible man-made or natural crises, while contributing to our competitiveness as set out in the report of Special Adviser Mario Draghi.

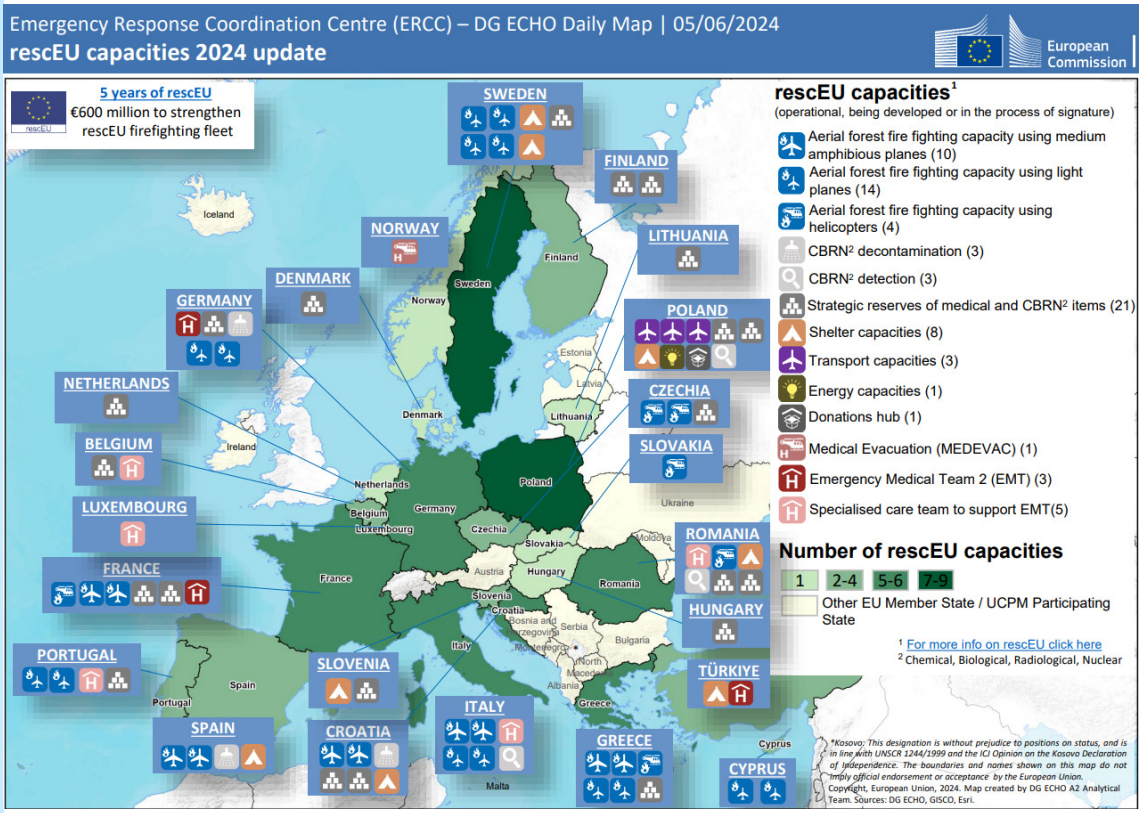
As part of its RescEU strategic reserve, the EU has started stockpiling medical countermeasures with a focus on CBRN threats, as well as other emergency and disaster response capabilities, such as emergency medical teams and medical evacuation planes, generators, emergency shelters and firefighting planes[07]. In the context of pandemic preparedness, the EU is also already developing a long-term strategy for the stockpiling of medical countermeasures and ever-warm manufacturing facilities to ensure preparedness beyond the current Multiannual Financial Framework. In addition, the Commission and Member States have recently developed a common strategic approach on medicines stockpiling to address shortages of critical medicines[08].

07. Established in 2019, rescEU represents the first-ever strategic reserve at the EU level, providing an additional layer of protection complementing Member States' capacities. Since 2019, EUR 3 billion have been invested, building up capacities in the area of CBRN (e.g. decontamination equipment), emergency shelter, energy (e.g. generators), medical emergencies (e.g. Emergency Medical Teams, medical evacuation planes), wildfires (e.g. Canadair firefighting planes), and transport and logistics. Currently, around 50 rescEU capacities are being hosted by 22 Member States and participating States.

08. European Commission, Communication on Addressing medicine shortages in the EU (COM(2023) 672 final/2), 2023.

FIGURE 7

Overview of capacities under the strategic rescEU reserve



Source: DG ECHO, 2024.

Stockpiling efforts in Member States and at the EU level were given a renewed impetus by Russia's invasion of Ukraine. Maintaining oil reserves for 90 days has been a long-standing practice across the EU. Building on this, the EU introduced regularly updated and binding targets for natural gas reserves in the 2022 Gas Storage Regulation, incentivising the purchase and management of strategic stockpiles by public and private entities. In addition, the 2023 Critical Raw Materials Act includes important actions to ensure a secure and sustainable supply of critical raw materials, and encourages stockpiling efforts at the national level.

Nevertheless, more needs to be done. Other major powers around the world, for instance the United States, China, Japan, and South Korea, are surging ahead and expanding strategic stocks of critical minerals and other resources as part of a broader effort to secure supply chains and ensure the resilience of key industrial sectors. For instance, in South Korea critical mineral stockpiles will be raised from 54 day-sufficiency to a 100 day-sufficiency target.

The EU and Member States need to take further steps in systematically developing such stockpiles and reserves – beyond ongoing efforts in the context of energy security, health preparedness, as well as emergency and disaster response. In this vein, Special Adviser Mario Draghi has already recommended the development of strategic stockpiles for selected minerals. To be fully prepared, a comprehensive approach to stockpiling involving both public and private actors is needed. The range of strategic resources and goods that are critical for preparedness and ensure the continuity of vital governmental, economic, and societal functions under all circumstances [see chapter 2] goes much further. For instance, this should include foodstuffs, basic chemicals (e.g. for water purification), or semiconductors, and even basic industrial components.

Despite the growing urgency to take action, the EU faces a number of challenges still hindering the development of a 'whole-of-society' approach to stockpiling, which should bring together the EU and Member States, as well as the public and private sectors in a coordinated effort. A recent proposal to

include provisions on the build-up of strategic reserves in the upcoming Internal Market Emergency and Resilience Act met strong opposition from Member States.

To make meaningful steps forward, the EU and Member States need to jointly address a number of challenges:

- **The issue of stockpiling remains sensitive**, with Member States perceiving it as one of their core competences in matters of national security. There are, therefore, strong reservations about the build-up of EU-level stockpiles, the setting of mandatory targets, and even a coordinated approach based on information sharing.
- **Levels of preparedness in terms of strategic stocks vary significantly across the Union**. On the one hand, this creates disincentives for Member States with already sufficient levels of stockpiles to enter into an EU-wide regime. On the other, Member States without such stocks would face additional costs in adjusting to an EU-wide regime. In general, Member States have been reluctant to share relevant data and information.
- For several strategic goods and resources, including critical raw materials, but also for oil, **the EU institutions still lack a comprehensive capacity to monitor in real time** supply chains, public and private stocks, and production capacities across Member States. The ability to quickly access and aggregate such information is essential to anticipating shocks and maintaining an agile stockpiling approach, catering for both public and private needs in Member States on an equitable basis.
- **Ultimately, this lack of EU-level information sharing reflects a wider need to build greater trust** between EU institutions, Member States, and the private sector. Trust is the main precondition for building a coordinated EU approach to stockpiling.
- Finally, meaningful action at the EU level, either by building up EU-level stocks or supporting Member States in reaching jointly agreed targets, will **require reflection on appropriate funding options**. Learning from the rescEU experience, these should not only address the build-up, but also the long-term maintenance of strategic reserves.

As the EU and Member States move to address these challenges, **there are a number of examples, both within and outside the EU, which can provide inspiration for a 'whole-of-society' approach to stockpiling**. For instance, with its National Emergency Supply Fund and the National Emergency Supply Agency (NESA), Finland has long-standing experience with emergency stockpiling, monitoring supply chain disruptions, and effective public-private cooperation. A recent government report on supply security highlights that Finland's stockpiles include compulsory reserves maintained by importers, as well as stockpiles for power and heating plants, pharmaceutical plants, and healthcare facilities. Similarly, Switzerland offers a model where the federal government, through the Federal Office for National Economic Supply (FONES), collaborates with the private sector to maintain compulsory stockpiles across four sectors: foodstuffs, energy, therapeutic products, and industrial products. These stockpiles are owned and managed by private businesses.

Other **valuable examples can be found among key partners, such as Japan and South Korea**. For instance, the Japan Organization for Metals and Energy Security (JOGMEC) is equipped with a broad mandate to identify industry needs and secure Japan's supply with critical minerals, including through strategic stockpiling. To this end, JOGMEC has developed strong intelligence capacities with a global reach, as well as access to a sizeable budget, and works closely with Japanese industry. The Japanese government supports JOGMEC's stockpiling efforts by covering the interest of the loans taken by JOGMEC to procure critical minerals, as well as the cost of maintaining warehouses.

Integrating preparedness-by-design into public procurement

The public procurement of goods and services is another dimension of public-private relations that warrants attention in the context of EU preparedness and resilience building. Every year, the more than 250,000 public authorities across the EU's Member States spend around EUR 2 trillion, or 14% of the EU's total GDP on the purchase of services, works and supplies. In many sectors, such as energy, transport, waste management, social protection and the provision[09] of health and education services, public authorities are the main customers[10]. Public procurement is therefore not only an essential instrument to ensure the smooth functioning of public services, but also to stimulate jobs, growth and investment; and to create an economy that is more innovative, resource and energy-efficient, and socially inclusive.

In this sense, **the design of public procurement rules has a significant impact on overall preparedness**. Depending on their nature and application, public procurement rules can have direct implications for the resilience of critical infrastructure, the continuity of vital functions, and by extension for the EU's economic security. Recent years have shown that it is necessary to assess how European public procurement procedures should be reinforced to explore how the logic of preparedness-by-design and related security considerations can be applied to public procurement to step up the resilience and protection of critical sectors, including telecommunications, transport, and energy, while keeping in line with the EU's international obligations under the WTO, and other bilateral investment treaties. As an instrument. While the recently adopted Financial Regulation Recast already provides a stronger legal basis (i.e. Article 136) to apply restrictions to EU award procedures in the case of an identification of security and public order risks, further steps are needed to ensure that public procurement at EU level and in Member States contribute to building public services and an economy that are more 'risk-proof' and resilient in case of unforeseen events.

09. European Court of Auditors, Public procurement in the EU, 2023

10. A separate Defence Procurement Directive (2009) was developed for the defence sector.

Recommendations

1. **Enhance public-private cooperation to facilitate resilience-building, as well as swift and coordinated responses to future crises:**

- × Develop stronger public-private information-sharing and coordination mechanisms to strengthen mutual and reciprocal exchanges on existing and emerging risks.
- × **Consider targeted and temporary flexibility measures, including further emergency derogations**, to better enable the private sector as a preparedness and crisis response actor, and to boost the security of supply for critical goods in crisis situations.
- × Systematically integrate private sector expertise in the development of preparedness policies and emergency planning.
- × Explore the application of the 'preparedness-by-design' principle in the context of the upcoming revision of the public procurement directive and related regulations.

2. **Reinforce private sector crisis preparedness and resilience:**

- × Raise businesses' awareness of the need for better preparedness and ensure a consistent level of crisis preparedness through joint public-private training and simulation exercises.
- × Extend the critical infrastructure resilience framework established under the CER and NIS2 directives to other crisis-relevant sectors, including notably Europe's defence industrial base.
- × Establish a targeted physical resilience framework for key manufacturing to enhance crisis preparedness and shock resistance.
- × Engage with businesses in institutionalising de-risking efforts, cross-sector stress tests and proactive security measures.
- × Establish industry-specific preparedness frameworks and sector-agnostic standards to mainstream resilience, preparedness and readiness planning in the private sector.

3. **Develop a comprehensive EU Stockpiling Strategy to incentivise coordinated public and private reserves of critical inputs, and ensure their availability under all circumstances.**

ENHANCE PUBLIC-PRIVATE COOPERATION FRAMEWORKS TO FACILITATE A SWIFT AND COORDINATED RESPONSE TO FUTURE CRISES:

→ Develop stronger public-private information-sharing and coordination mechanisms to strengthen mutual and reciprocal exchange on existing and emerging risks.

Leveraging the full potential of public-private cooperation and improving overall EU preparedness and readiness requires tackling gaps in communication and coordination between public authorities and private entities. Private companies and operators in critical sectors often do not receive timely and adequate information – both in terms of early warning and operational guidelines on dealing with a threat – from public authorities. In turn, this delays vital information dissemination and resource allocations, which can have economic repercussions and undermine the overall crisis

response of Member States and the EU. At the same time, a lack of trust and effective information-sharing tools keeps private companies from notifying vulnerabilities and incidents adequately, and delays action by public authorities.

To overcome these hindrances, it is crucial to reinforce secure information-sharing mechanisms and standardised protocols, enabling systematic information sharing between businesses and Member States' competent authorities, as well as between Member States authorities and the relevant EU institutions, bodies and agencies.

At the same time, both the public and private sectors share a responsibility to be more proactive in their information sharing. Secure and trusted systems should enable companies to notify incidents and to share sensitive information about vulnerabilities, while allowing Member States to warn and regularly update businesses and operators about existing threats. This requires not only technical means, but procedural agreements, including the ability to receive and process such information.

In addition, public authorities should proactively leverage voluntary information and coordination frameworks to build trust with the private sector and establish dependable working relationships that are vital in crises. To this end, the EU and Member States should build on the positive experiences of close public-private coordination during the COVID-19 pandemic, including at the EU level, in several sectors of our economies.

→ **Consider targeted and temporary flexibility measures, including further emergency derogations, to better enable the private sector as a preparedness and crisis response actor, and to boost the security of supply of critical goods in crisis situations.**

Flexibility can be essential to enable the private sector to take rapid action and to support public authorities' crisis response under a 'whole-of-society' approach. In particular, this concerns the private sector's capacity to maintain and scale up the EU's supply with essential goods during crises. To this end, the EU could consider targeted flexibility measures to better enable the private sector as a crisis response actor. Such measures could include:

- **Further developing emergency provisions and derogations in relevant product and other legislation to temporarily suspend clearly specified regulatory requirements during emergencies to facilitate rapid and effective response and meet emergency needs.** For instance, this could follow the example of the new legislation on standards of quality and safety for substances of human origin (SoHO) intended for human application. The revised regulation includes important provisions to ensure supply continuity, such as providing SoHO blood and blood components during armed conflicts and dealing with sudden increases in demand. The Regulation now allows for flexibility during crises. Member States can use derogations from certain provisions when needed to mitigate risk to human lives during large-scale life-threatening disasters, whether natural or man-made. In a similar vein, the EU could comprehensively screen existing legislative and institutional frameworks – not only in the area of health – to identify bottlenecks and specific issues, where targeted derogations applicable in crisis situations could contribute to preparedness and accelerate public-private cooperation in responding to crises. For instance, building on this screening, the EU and Member States could then reflect on the need to introduce provisions for lowering – on a case-by-case basis – product quality standards in crisis situations. This should also lead to reflections on a selected, case-by-case basis. In addition, to ensure the rapid scale-up of the manufacturing of critical crisis goods, such as Personal Protective Equipment (PPE), the EU should make sure that private partners can readily access certified product blueprints to scale up production in line with the right design standards.

- **Formalising tried-and-tested ad hoc public-private crisis cooperation arrangements with the Commission that emerged as part of the EU's response to the COVID-19**

pandemic and Russia's war of aggression against Ukraine. Such successful formats enabled the acceleration of the development and authorisation of treatments and vaccines. Another best practice was the inclusion of industry representatives in the Gas Coordination Group, which facilitated essential public-private coordination during the energy crisis. The pilot project channelling private sector donations via the Union Civil Protection Mechanism and rescEU to Ukraine is another successful example. Finally, the EU could also build on pandemic-era ad hoc derogations from State aid rules to develop a more structured and anticipatory approach to derogations in times of crisis.

BOX 7

Health Preparedness - vaccine development and distribution

Public-private partnerships have proven to be a cornerstone in bolstering health preparedness, particularly evident in the rapid development and distribution of vaccines. The unprecedented global challenge of the COVID-19 pandemic underscored the necessity for cohesive action between governmental bodies and pharmaceutical companies. This collaboration facilitated the sharing of resources, expertise and data, accelerating vaccine research and ensuring swift regulatory approval processes. The success of these partnerships has set a precedent for tackling future health emergencies, demonstrating the efficacy of combining public oversight with private sector innovation.

The EU's strategy for vaccine development, manufacturing, and distribution serves as a testament to the strength of public-private cooperation. Initiatives such as the Advanced Purchase Agreements provided the necessary funding and market guarantees that incentivised companies to invest in vaccine research and production capacity. This approach not only spurred the rapid development of multiple vaccines, but also ensured that Member States had equitable access to these life-saving resources . The EU's joint procurement strategy exemplified the benefits of a coordinated approach, leveraging collective bargaining power to secure vaccines for the entire Union and avoid harmful competition between Member States.

To further enhance the resilience of health systems, the EU is expanding public-private partnerships beyond vaccine development, for instance as part of the Innovative Health Initiative, to encompass the entire spectrum of medical countermeasures, including therapeutics and diagnostics. By fostering an environment conducive to long-term investment in research and development, the EU can ensure a steady pipeline of innovative health solutions. This requires a clear regulatory framework that balances the need for rapid response during emergencies with the maintenance of high safety and efficacy standards.

Moreover, the distribution of vaccines highlighted the importance of robust logistics and supply chain management, areas where the private sector's expertise was invaluable. Future public-private partnerships should focus on building and maintaining resilient supply chains that can withstand disruptions caused by health crises and other emergencies. This includes diversifying manufacturing sites and raw material sources, as well as investing in cold chain infrastructure to ensure the integrity of temperature-sensitive products. Public-private cooperation in health preparedness should also not be limited to crisis response, but encompass prevention and early detection enhancing EU's anticipatory capabilities.

→ Systematically integrate private sector expertise in the development of preparedness policies and emergency planning.

To strengthen the preparedness and readiness of EU businesses, it could be valuable to integrate private sector expertise more systematically into public planning, for example at an earlier stage in the development process of preparedness policies and emergency preparedness plans. This would enable policy-makers to better tailor policies to the needs and capabilities of critical private sector actors and enable them to cooperate more effectively with public authorities in crisis response. The European Commission's 'Have Your Say' platform already provides a basic framework for public consultations where businesses can contribute their insights to the legislative process. However, this approach could be significantly improved by developing more interactive and continuous engagement mechanisms to ensure that businesses can provide feedback and innovative solutions to emerging challenges. Building on existing approaches, such as the Industrial Forum for business consultations, Commission Directorates-General could further institutionalise this engagement by developing 'Know Your Business Counterpart' approaches, for example using data from the EU Transparency Register, which currently lists over 12,800 organisations[11]. This could facilitate targeted consultations with businesses to ensure that their expertise is effectively used in shaping EU policies where strong preparedness depends on functioning cooperation with the private sector.

→ Explore the application of the 'Preparedness-by-Design' principle in the context of the revision of the Public Procurement Directive and related regulations.

In line with the European Commission's 2021 report on the implementation of Directive 2014/24/EU on public procurement, there is significant room for improvement in the effective and efficient application of EU public procurement rules in Member States. This also creates latitude for a more rigorous integration of strategic considerations into the debate on wider public procurement reform. A wider review, including the 2014/24/EU Public Procurement Directive, but also Directive 2014/23/EU on the award of concession contracts or Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors, should therefore analyse their interdependent network approach and align it further with the priorities set out in the Political Guidelines (2024-2029) and the Mission Letters of the incoming College of Commissioners. In line with these priorities, the review should make the public procurement process simpler and faster, and fit for purpose in light of new challenges and risks linked to preparedness, economic security, critical infrastructure resilience, and defence. This would also be in line with the Council Conclusions of May 2024[12], which called for improving effective competition in EU public procurement for works, goods and services, while highlighting the importance of clear rules on the treatment of products and economic operators from third countries.

2. REINFORCE PRIVATE SECTOR CRISIS PREPAREDNESS AND RESILIENCE:

→ Raise awareness of the need for better preparedness and ensure a consistent level of crisis preparedness through joint public-private training and simulation exercises.

Training, exercising and other awareness raising instruments would be crucial to ensure a consistent level of preparedness across the private sector, to share best practices in public-private crisis coordination, and encourage cross-company and cross-sector cooperation. For instance, the creation of EU-level courses – institutionalised in the framework of an EU Academy – or large-scale joint exercises, could prove beneficial in bringing together a variety of stakeholders across the Single

11. European Commission, Transparency Register, 2024.

12. Council of the European Union, Competitiveness Council meeting (24 May 2024) – Conclusions, 2024.

Market. This could include representatives from public administrations, the private sector, critical infrastructure entities, and civil society [see the recommendations on exercising and training in chapters 2 and 3].

Such training and exercising programmes could also be useful to support private companies in developing their own crisis preparedness plans addressing critical issues, such as the stockpiling of raw materials and other critical inputs, supply chain diversification pathways, and labour shortages. Enhanced public-private cooperation on these plans could help to identify critical needs and to stimulate joint investment in common infrastructure and capabilities critical for preparedness purposes. This could, for instance, build on the example of EU-FAB, a framework contract with six economic operators establishing a network of ever-warm production capacities for vaccine manufacturing. This allows sufficient and agile manufacturing capacities for different vaccine types to be kept operational, ready for quick activation in the event of a public health emergency. Such mechanisms are crucial for the EU to respond swiftly and autonomously to future emergencies.

→ Extend the critical infrastructure resilience framework established under the CER and NIS2 Directives to other crisis-relevant sectors, including notably Europe's defence industrial base.

To complement the resilience frameworks at Member State level established through the implementation of the CER and NIS2 Directives, which provide a basis for protecting critical infrastructure against a wide range of threats, from cyberattacks to natural disasters, it could prove beneficial to explore broadening the sectoral scope of the current EU legislative framework to other critical sectors and industries vital to the maintenance of core governmental, societal, and economic functions in line with the Treaties. For instance, the defence industry should be equipped with robust risk management and crisis response capabilities, building on the extensive experience these companies have with managing security threats.

To facilitate the process, focus could be placed on harmonising and consolidating existing instruments to make them more effective and inclusive of these additional sectors at the same time. Member States and their intelligence and security services should be enabled to work closely with the European Commission, IT services and private sector actors to standardise resilience strategies, ensure consistent implementation across the Union, and to facilitate information sharing. Furthermore, complementing scope, the EU could promote greater coherence in its approach to critical infrastructure protection, ensuring that all sectors, especially those related to defence and other high-risk areas, are adequately protected, to maintain the integrity and continuity of critical services in all Member States under all circumstances.

→ Establish a targeted physical resilience framework for key manufacturing to enhance crisis preparedness and shock resistance.

Private sector companies are vital partners in ensuring the continuity of the EU's vital functions (as developed in chapter 2). With the CER and NIS2 directives, the EU and Member States have already taken an important (cross-)sectoral approach to stepping up the resilience of critical entities that ensure the provision of essential services in key sectors, such as energy, transport, digital and space. In addition, action has been taken to ensure the security of supply for the Internal Market with the Internal Market Emergency and Resilience Act, alongside a wide array of sectoral legislation.

Apart from entities that provide essential services, comprehensive preparedness requires the resilience of manufacturing, especially when looking at major crises, including armed aggression. The production of highly specialised goods, such as semiconductors, aircraft and spacecraft, communications and security equipment, and specialised machines and vehicles needs to be ensured in times of crisis. While manufacturing is covered by the cybersecurity rules of NIS2, it is not included in the framework for physical resilience under the CER Directive. In the recent past, there have been several incidents of the physical sabotage of manufacturing in the EU. In the event of escalating geopolitical crises, the EU's vital manufacturing infrastructure – a key preparedness resource – could become a prime target.

In addition, some manufacturing companies may acquire a particular systemic importance – either because of their size, their pivotal position within a complex supply chain or business network, their geographical position and spread, or their cross-border relevance. Due to their systemic importance, the disruption of such companies caused by external shocks – from natural disasters and cyberattacks to geopolitical tensions and supply disruptions – could lead to cascading failures across the economy, and ultimately pose a real threat to the continuity of vital functions.

To further 'crisis-proof' the Single Market and ensure the continuity of critical economic activity during crises, the EU and its Member States should extend on a targeted (company-level) basis existing resilience-enhancing frameworks to manufacturing, in doing so supporting key players that help to ensure the EU's vital functions. To this end, a methodology drawing on economic and company-level data could be developed to map linkages, dependencies and supply chain networks for manufacturing to identify key 'node points' whose disruption could have cascading effects on the wider economy. Having identified manufacturing of systemic importance, Member States should work closely with these actors, providing access to measures that enhance their resilience and their ability to deliver goods and services. For instance, Member States could make use on a voluntary basis of measures and instruments on physical resilience, as they are foreseen for critical entities under the CER Directive and the cooperation framework used for critical infrastructure at the EU level. Furthermore, the EU and Member States could design additional measures to strengthen their security of supply. For instance, this could include financial incentives to encourage the build-up of stockpiles of spare parts and raw materials, or to diversify suppliers.

BOX 8

Energy infrastructure resilience - addressing future vulnerabilities

The EU faces significant challenges in ensuring the resilience of its energy infrastructure to future vulnerabilities, ranging from cyberattacks, to natural disasters and geopolitical tensions. Public-private cooperation has emerged as a crucial element in enhancing the robustness and security of the energy sector. By leveraging the strengths and resources of both the public and private sectors, the EU can create a comprehensive approach that not only addresses immediate threats, but also anticipates and mitigates future risks.

Enhancing cybersecurity measures: As energy infrastructure becomes increasingly digitised and interconnected, the threat of cyberattacks grows more pronounced. Governments and the EU can provide regulatory frameworks, information on the threat landscape and incentives for additional means to enhance cybersecurity, while private companies can provide technical expertise and innovative solutions. For example, collaborative initiatives such as the European Energy – Information Sharing & Analysis Centre (EE-ISAC) allows both public and private actors to stay ahead of cybercriminals to protect the integrity of energy networks.

Investment in smart grid technologies: The transition to smart grids is another key aspect, as they incorporate advanced sensors, automation, and real-time data analytics to optimise the production, distribution, and consumption of energy. For instance, the EU's Horizon Europe

programme provides significant funding for research and innovation in smart grid technologies, while private sector entities invest in the development and implementation of these systems.

Addressing physical and geopolitical risks: These include natural disasters and political instability. Governments can lead in identifying strategic vulnerabilities and in setting resilience standards, while private companies can focus on implementing these measures and investing in resilient infrastructure. For example, the construction of more robust and flexible energy networks can help to mitigate the impact of natural disasters, while diversifying energy sources and supply routes can reduce dependency on geopolitically unstable and rival regions.

Promoting innovation and resilience culture: EU programmes like the European Innovation Council (EIC) fund cutting-edge projects that aim to enhance resilience. Fostering a culture of resilience involves training and educating all stakeholders, from policy-makers to engineers and the public about the importance of preparedness and adaptive strategies.

Collaborative policy and regulation development: Collaborative efforts between the EU, national governments and private sector entities can lead to the development of comprehensive policies that address current and future vulnerabilities. This includes creating standards for cybersecurity, mandating regular risk assessments, and ensuring compliance with resilience measures. Inclusive policy-making also promotes economic security and sustainability.

→ Engage with businesses in institutionalising de-risking efforts, cross-sector stress tests and proactive security measures.

Building on previous successful examples of public-private cooperation, such as the energy sector stress-tests, the EU and Member States should further roll out and institutionalise stress tests and de-risking efforts across sectors by systematically engaging with and encouraging businesses to go beyond the legally required minimum. Likewise, it is of the utmost importance that critical projects for the Union are meticulously planned and screened to avoid the creation of new vulnerabilities.

Furthermore, in the spirit of a 'whole-of-society' approach, it is essential to engage businesses, and particularly small and medium-sized enterprises, in actively integrating their employees and conducting regular security awareness and training initiatives.

To support companies in implementing preparedness and resilience measures, for instance in the context of economic security, the EU should proactively provide integrated data and analysis to support the development of corporate adjustment strategies. Building on the NIS-2 Directive, which already provides a framework and legal basis for EU coordinated risk assessment of supply chains, the EU should continue to assess and review the security of the supply chain architecture of different sectors, with a view to moving from a siloed approach to an integrated, collaborative framework across the Commission's Directorates-General (DGs), in cooperation with the whole ecosystem of stakeholders relevant to preparedness and readiness. This needs to extend from energy producers to infrastructure operators, critical raw material suppliers in the manufacturing industry, health service providers, and beyond.

BOX 9

Subsea Preparedness - promoting security under water

More than 95% of global internet traffic between continents is carried by undersea cables that stretch across the ocean floor. These cables are owned by a mix of private and State-owned organisations. The EU is in the process of laying down various cables under the Global Ring, such as the Arctic Cable.

The security and resilience of the EU's network and computing infrastructure is an essential element of our digital autonomy. In line with the White Paper and the EU Recommendations of February 2024, an EU governance system for submarine cable infrastructures could be established, including:

- Measures to mitigate and address risks, vulnerabilities and dependencies in the context of a consolidated EU-wide assessment, and priorities for increasing resilience.
- A revision of the criteria for upgrading existing cables or funding new ones, with an update of the jointly established priority list of cable projects of European interest.
- Adequate funding from the CEF for Cable Projects of European Interest (CPEIs) and the pooling of EU and national funding instruments, and exploring the feasibility and potential leverage of financial instruments, as possible delivery modes to ensure synergies and sufficient funding for CPEIs.
- Further measures to secure supply chains and avoid reliance on high-risk third country suppliers. Member States may also consider whether the deployment and operation of certain CPEIs may require further public support in line with State aid rules, support through the purchase of capacity for public use, or whether some adjustments to EU market regulation may be necessary to ensure that the whole value chain is built by secure EU-owned companies.
- The establishment of a common EU fleet for maintenance and repair, for example through a Joint Undertaking. This work stream could learn from the experience of the Union's Civil Protection Mechanism and RescEU, in particular regarding firefighting; and from other EU agencies, such as FRONTEX and the European Maritime Safety Agency (EMSA).
- The harmonisation of security requirements, including through the identification of best standards taking advantage of the latest developments in security and self-monitoring capabilities for cables and associated routing and relay equipment, which could be recognised through a dedicated EU certification scheme.
- Strengthening cooperation with NATO and like-minded partners on the issue could provide additional means and help to share the costs of improved subsea preparedness.

→ **Establish industry-specific preparedness frameworks and sector-agnostic standards** to mainstream resilience, preparedness and readiness planning in the private sector. The aim is to ensure that companies are better equipped to anticipate, respond to and recover from disruptions, safeguarding their long-term viability and resilience. This mainstreaming could be systematically promoted when new EU legislation is proposed, or when existing legislation of the EU acquis is revised. When new legislative initiatives are proposed, these should include appropriate requirements or incentives for businesses to integrate such planning efforts into their operations, while establishing flexibilities to respond and react in times of crisis or in case of unforeseen events.

This would also be in line with the 'security and preparedness check' recommended in chapter 2. Before releasing new initiatives, the Commission could conduct a comprehensive check as part of the Better Regulation Toolbox to ensure that new legislative proposals support the strategic integration of resilience measures into corporate strategies. This would better equip businesses to cope with potential disruptions, thereby improving their overall economic performance and sustainability. Integrating these practices could not only reduce risks, but also create competitive advantages, contributing to a more resilient, stable and competitive EU economy.

3. DEVELOP A COMPREHENSIVE EU STOCKPILING STRATEGY TO INCENTIVISE COORDINATED PUBLIC AND PRIVATE RESERVES OF CRITICAL INPUTS, AND ENSURE THEIR AVAILABILITY UNDER ALL CIRCUMSTANCES:

The EU needs to be better able to absorb shocks, disruptions and supply/price volatility to ensure its capacity to function under all circumstances. Current trends of geopolitical friction, securitisation and tensions are expected to continue. While fully acknowledging Member States' role in the domain of stockpiling and strategic reserves, joint action at the EU level could help to strengthen the EU's strategic autonomy and contribute to the de-risking of excessive external dependencies in terms of raw materials and other crisis-relevant goods. This should be closely connected to the wider efforts to diversify supply chains and reduce vulnerabilities.

As a long-term objective, an integrated system of cross-sectoral strategic reserves should be developed, linking the EU level, Member States and the private sector. For instance, this could build on the rescEU model. In the short- to medium-term, building on the Draghi report's recommendation for joint stockpiles of critical minerals, an EU Stockpiling Strategy could propose a step-by-step approach:

- **Systematically map ongoing efforts and best practices** within the EU and among key partners and major global powers. For instance, engagement with countries that face similar dependency challenges and have developed specific institutional models (such as Japan and South Korea) could provide valuable insights and lessons for improving preparedness and exploring possibilities for a coherent EU approach to strategic stockpiling.

- Undertake a **joint needs and capabilities assessment** with a view to enabling Member States to better coordinate and prioritise the build-up of stockpiles and emergency reserves, and ensure an even level of preparedness across the Union. To address the challenge of trust and information sharing, the EU and Member States could start by cooperating in smaller groups who share particular challenges or interests and/or explore the establishment of a secure coordination and information-sharing platform capable of handling classified information.

- Building on existing EU-level efforts, **jointly identify a comprehensive set of categories of essential inputs** (e.g. foodstuffs, energy, critical raw materials, emergency response equipment, medical countermeasures) and **define targets to ensure minimum levels of preparedness** in different crisis scenarios, including in the event of an armed aggression or the large-scale disruption of global supply chains. **Targets should be regularly reviewed and updated** in light of supply chain monitoring (already foreseen under sectoral legislation, such as the Chips Act, the Critical Raw Materials Act, the pending European Defence Industrial Programme, the Emergency Framework to ensure the supply of crisis-relevant medical countermeasures, or the Internal Market Emergency and Resilience Act), intelligence assessments, and the comprehensive EU Risk Assessment [see chapter 2].

- **Ensure coherence and coordination between future initiatives and ongoing EU-level stockpiling efforts**, such as in the field of health preparedness, disaster and emergency response, energy and critical raw materials.

- **Strengthen the EU's ability to monitor in real time** critical supply chains, production capacities, as well as public and private stocks of select items and resources to ensure a sufficiently agile approach to stockpiling.

- **Build an enhanced public-private partnership** based on trust and mutual information sharing. There needs to be a shared understanding between EU institutions, Member States and the private sector that we have a common interest in strengthening the EU's resilience to supply chain shocks

and other disruptions. The security of information sharing and the confidentiality of its handling by all involved parties needs to be ensured.

- **Develop a set of operational criteria to guide the coordinated release of emergency reserves** and stocks during emergencies or supply disruptions.
- **Explore options to replenish strategic reserves through joint procurement and identify innovative financing options to incentivise the build-up and long-tern maintenance** of public and private stockpiles, for instance by covering the interest of the loans taken to procure stocks as in the Japanese case or sharing the costs of maintaining the additional production capacity of ever-warm facilities for crises situations.

CHAPTER · CHAPTER · CHAPTER

06

Outsmarting malicious actors to deter hybrid attacks

Responding to a growing threat

Malicious hybrid campaigns are designed to destabilise, weaken and divide the EU and its Member States. They are a serious threat to our security and the EU must further strengthen its capacity to counter them. These hybrid threats refer to actions by State and non-State actors that **seek to exploit vulnerabilities** to their own advantage by using – in a coordinated way – a mixture of coercive and subversive activity, with conventional and unconventional methods, while remaining below the threshold of overt conventional warfare[01].

The methods of hybrid operations evolve constantly, and the EU and its Member States are currently targeted by a hybrid campaign that involves sabotage, cyberattacks, economic coercion, the jamming and spoofing of satellite signals, the instrumentalisation of migrants, Foreign Information Manipulation and Interference (FIMI), as well as political infiltration. Hybrid operations' methods are **inherently ambiguous, subversive and difficult to detect, often exploiting global connectivity and supply chains, economic dependencies, legal loopholes, internal political divisions or the openness of our democratic societies**[02]. Hybrid campaigns by malicious State actors are often planned and organised by malicious foreign intelligence services and combined with illegal espionage activities, while individual acts are often carried out by proxies.

01. European Commission and High Representative, Joint Framework on Countering Hybrid Threats: A European Union response (JOIN(2016) 18 final), 2016.

02. They include cyber-hacks, FIMI, elite capture, espionage, coercion technology acquisition by legal and illegal means, strategic foreign direct investments through companies tied to the government, transnational repression and related pressure campaigns on journalists, activists, researchers, companies, etc.

The EU has already taken steps to build preparedness and resilience against hybrid threats, starting with the 2016 Joint Framework on Countering Hybrid Threats, that set up a broad array of measures – covering prevention, preparedness and response – in a substantial number of policy areas[03]. For instance, this included an EU Hybrid Toolbox to ensure a coordinated response to hybrid campaigns, an FIMI Toolbox bringing together a set of tools to counter Foreign Information Manipulation and Interference (FIMI), the EU Cyber Diplomacy Toolbox, a set of restrictive measures to respond to cyberattacks and other malicious activities in the cyber realm. In addition, the EU and Member States are undertaking efforts to step up the physical and cyber resilience of our critical infrastructure [see chapter 5][04], and have developed enhanced capacity to conduct joint investigations into suspected hybrid operations [see Box 11 on counter-sabotage]. Most recently, the EU adopted a new sanctions framework against those responsible for destabilising activities against the EU and its Member States – responding in particular to Russia's intensifying hybrid operations[05].

However, the significant increase in the number of malicious activities on the EU's territory this year points to the increasingly brazen and aggressive nature of hybrid activities by external actors, in particular, but not only Russia. Certain malicious activities, such as acts of (physical) sabotage or cyberattacks, may not only disrupt economic, energy, transport or digital networks, but can also cause possible cascading effects across other sectors and even lead to the loss of human life. Other hybrid activities – such as Foreign Information Manipulation and Interference (FIMI) or political infiltration – have a corrosive long-term effect on society, for instance supercharging political polarisation, and contributing to a political climate increasingly conducive to acts of political violence and extremism [see chapter 4][06].

These recent developments underline the urgency for the EU to step up its preparedness and resilience against the full spectrum of hybrid threats. So far, the EU's increasing efforts to prevent, prepare for and respond to hybrid actions have been insufficient to credibly deter **threat actors, who consider** that they can act at little cost and with relative impunity. If the EU and Member States want to further limit the number and impact of hybrid attacks, they **need to become faster and more assertive in their response**.

While keeping fully in line with the democratic principles and values of open societies and respecting EU, national and international law, **we should strengthen the ways in which we deter, prepare for and address the ruthless and increasingly reckless behaviour of these threat actors. This is all the more important in anticipation of a possible escalation of hybrid campaigns in the future**.

BOX 10

Securing Europe's borders – Belarus' instrumentalisation of migrantsThe increasing scope and intensity of hybrid threats

Especially in 2021, but also today, Poland, Latvia and Lithuania have experienced high pressure via their external borders with Belarus. These arrivals were concerted by Belarussian authorities as part of wider hybrid attacks to undermine the national security of affected Member States. For the Commission, it was key to support the Member States affected using the legal, financial and operational tools available.

03. This includes the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, as well as the announcement of a new approach based on mainstreaming hybrid threat considerations into all policy initiatives as part of the 2020 Security Union Strategy (COM(2020) 605 final). Further measures were taken with the establishment of the EU Cyber Diplomacy Toolbox, the EU Hybrid Toolbox and the EU FIMI Toolbox, which include tailored measures to ensure an integrated, strategic, operational and systematic approach to malicious activities targeting the EU, its Member States and partners.

04. Notably through the adoption of the Critical Entities Resilience (CER) Directive and the NIS2 Directive on cybersecurity.

05. See: Council of the European Union, New sanctions framework against those responsible for destabilising activities against the EU and its Member States, 2024.

06. Ahead of the European Parliament elections in June 2024, the EU experienced an unprecedented surge of political violence – often linked to the extreme right – targeting elected politicians and candidates. Several Member States, including especially Germany, but also Slovakia, Denmark, the Netherlands, Poland, and France were affected.

Legal measures available in the situation of instrumentalisation include – under specific circumstances – border closures, as defined in the Schengen Borders Code. From June 2026 onwards, the Crisis and Force Majeure Regulation as part of the Pact on Migration and Asylum will provide for a comprehensive crisis framework at the EU level, including a derogation allowing affected Member State to apply the border procedure to everybody, while ensuring the respect for fundamental rights. Beyond this, provisional measures in emergency situations characterised by a sudden inflow of third-country nationals can be adopted based on Article 78(3) TFEU.

To support the three Member States affected by the situation at the Belarussian border in 2021, the Commission made available financial support of approximately EUR 200 million via Specific Actions – in the case of Lithuania, also under Emergency Assistance. Furthermore, to enhance the border surveillance capabilities of Member States that share an external border with Russia and/or Belarus, as cases of the instrumentalisation of migrants and asylum-seekers continue to occur, the Commission recently published a call for a Specific Action under the Thematic Facility of the Border Management and Visa Instrument, with a budget of EUR 150 million.

Support to said Member States was also provided operationally and on the ground. Via the Blueprint network, the Commission was monitored the situation closely. The Commission also reached out successfully to Iraqi authorities to interrupt flights between Iraq and Belarus. According to data provided by Member States, this led to an 83% reduction in irregular border crossings and to a 35% reduction in attempts to cross at the external border with Belarus in 2022 compared to 2021. In addition, Europol, the European Union Agency for Asylum (EUAA) and Frontex provided and continue to deliver operational support to the Member States concerned. As of May 2024, Frontex is present in all three countries, Europol is present in Lithuania and Poland, and the EUAA is present in Lithuania.

The increasing scope and intensity of hybrid threats

Hybrid threat actors are **increasing the scale and intensity of their hybrid operations within the EU**, while ramping up hybrid campaigns as a way to gain influence and interfere with the EU's interests in third countries and regions[07].

In particular, malicious cyber activities as an attack vector have reportedly risen significantly in recent years[08]. To a large extent, these seem to be connected to geopolitical tensions. In carrying out cyberattacks, State actors increasingly use individuals and other proxies. In addition, the increasing digitalisation of our societies and economies and the accelerating emergence of disruptive technologies have created and will continue to create more vulnerabilities, and expand the attack surface for malicious actors. Malicious cyber activities often have consequences in the physical world, causing significant damage in numerous vital sectors, including health, financial services, transport and energy.

At the same time, especially since 2023, there has been a **marked increase in the number of (attempted) acts of physical sabotage across the Union**[09]. For instance, German authorities were

07. RUSI, The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022–24, 2024.

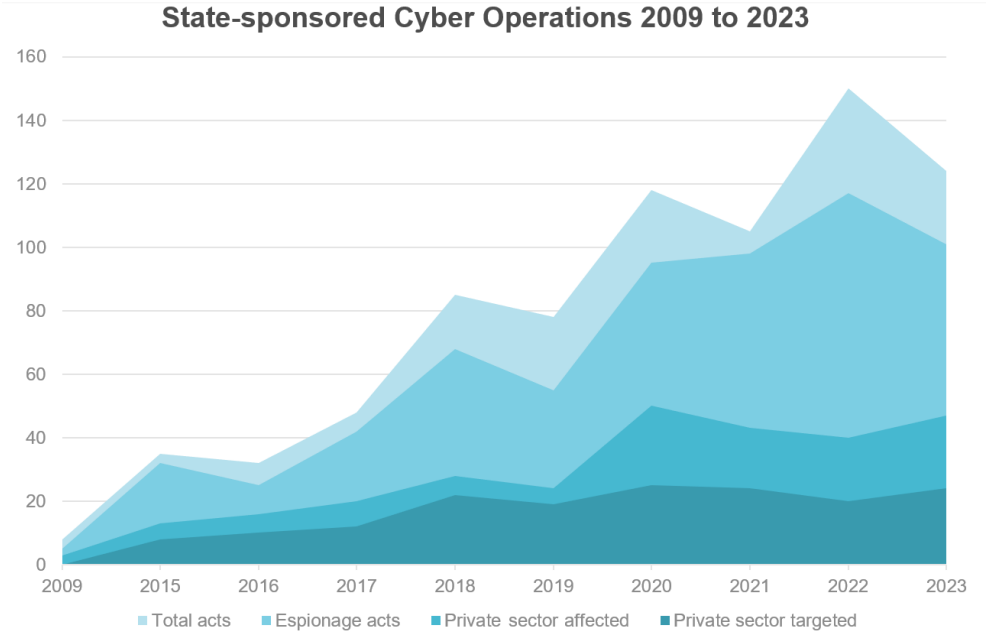
08. According to the European Union Agency for Cybersecurity (ENISA), the number of observed malicious cyber incidents in the EU has significantly increased between the second half of 2022 and the first half of 2024. Between July 2022 and June 2023, ENISA reported slightly more than 2,500 reported incidents. Instead, between July 2023 and June 2023, ENISA reported more than 5,000 observed incidents. See: European Union Agency for Cybersecurity, ENISA Threat Landscape, 2023. See: European Union Agency for Cybersecurity, ENISA Threat Landscape, 2024.

09. Politico, Russian espionage, sabotage in Europe now 'more likely,' Norwegian intel chief warns, 2024.

able to foil a suspected Russian plot involving explosives and arson attacks on military and industrial facilities in April 2024. Similarly, in 2023 Polish authorities arrested members of an alleged Russian spy ring planning to derail a train carrying aid to Ukraine.

FIGURE 8

Increase in State-sponsored cyber operations worldwide



Source: EUISS, 2024, based on data from the Council on Foreign Relations, Cyber Operations Tracker, 2024.

The distinct nature of different hybrid actors and their tactics further complicates the picture. **We need to increasingly take into account that their respective historical traditions, doctrines, interests, aims and capabilities shape the way different State and non-State hybrid actors operate. At the same time, different malicious actors are increasingly learning from each other**[10]. Threat actors already amplify each others' efforts and there are strong grounds to expect converging cooperation, even if that doesn't (yet) mean 'joint' hybrid operations. Vulnerabilities to one actor (for example, in the economic, cyber, or infrastructure domain) could also lead to potential vulnerabilities to other actors. These threat actors analyse the EU's reactions to hybrid campaigns by other perpetrators when assessing their own methods, as well as the risks of detection and countermeasures, adapt their methods accordingly.

BOX 11

Protecting Europe's critical infrastructure from sabotage

Sabotage, the intentional disruption of facilities or systems necessary for delivering essential services, such as energy, health, transport, communication or water, is a domain at the very core of Member States' security. Given the increasing use of sabotage by hostile third countries, notably Russia, it is an area where internal security and military security are very much interlinked. From a prevention, preparedness and response angle, effective cooperation between law enforcement, intelligence authorities, military and civil protection, and private operators is essential.

10. European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE Research Report 8: Russia and China as hybrid threat actors: The shared self-other dynamics, 2023.

Counter-sabotage has long been excluded from meaningful EU-level cooperation due to its sensitivity as a matter of national security. The Russian war of aggression against Ukraine has, however, shifted the approach. Counter-sabotage has now become a central pillar of the cooperation on critical infrastructure and in the context of countering hybrid threats at the EU level, including work with key partners, such as NATO and Ukraine. A number of key milestones are listed below:

- **Since February 2022:** Deployments of Protective Security Advisory Missions to support Member States' vulnerability assessments of critical infrastructure.
- **December 2022:** Adoption of the Council Recommendation on a Union-wide approach to strengthen the resilience of critical infrastructure.
- **January 2023:** Entry into force of the Directive on the Resilience of Critical Entities and the NIS2 Directive on cybersecurity in the EU.
- **January 2023:** Beginning of the resilience stress test in the energy sector, completed in April 2024.
- **June 2023:** First EU-NATO Parallel and Coordinated threat assessment for critical infrastructure.
- **July 2023:** First assessment report of the EU-NATO Task Force on the resilience of critical infrastructure.
- **October 2023:** Activation of the Hybrid Toolbox by Finland after the Baltic connector incident.
- **May 2024:** Adoption of the Critical Infrastructure Blueprint.
- **June 2024:** Activation of the Hybrid Toolbox by Lithuania, Poland, and the Czech Republic after numerous sabotage cases.
- **October 2024**: Entry into application of the Directive on the Resilience of Critical Entities and the NIS2 Directive on cybersecurity in the EU.

These experiences have shown that there does not have to be a dichotomy between Member States' responsibility for security and cooperation at the EU level, but rather that a combination provides the best possible response.

Strengthening our comprehension of the threats and threat actors

Enhanced EU preparedness against hybrid threats needs to create a higher threshold for malicious actors to engage in hostile activities against us by strengthening our deterrence. There are two main dimensions:

- First, **deterrence by denial**, which means that the potential perpetrator is discouraged from malicious activities against the EU, because they know that the EU is able to protect itself to an extent that no hybrid campaign is likely to reach its objectives.
- Second, **deterrence by punishment**, which means that the potential perpetrator is dissuaded from further operations, as they come to the conclusion that the response from the EU will be so decisive and the consequences so costly that it outweighs any potential benefits of continued hybrid operations.

→ Deterrence by denial

To create deterrence by denial, we must strengthen the EU's capacity for prevention, its ability to increase the resilience of potential targets by tackling vulnerabilities, and capacity for effective damage mitigation and consequence management.

As a first step, effective deterrence by denial requires us to understand the ways in which threat actors behave and how their methods are evolving. For this reason, the EU must be better able to take advantage of intelligence and situational awareness analysis in policy planning and decision-making processes.

To reduce the number of weak spots for malicious influencing, the EU and **Member States should build on ambitious efforts across different sectors, including media freedom and disinformation, cybersecurity and many others. It should continue to agree on common legislative and operational measures to make it as difficult as possible for malicious actors, including hostile foreign intelligence services, organised crime, and terrorist organisations, to operate within the EU's territory**. All Member States have an equal responsibility to regularly assess their vulnerabilities across all levels of government and society, and to ensure that their own legislative and organisational frameworks allow them to address these weak spots fully. Even one weak link in the chain exposes all other Member States to the threats as well, if a malicious actor is, for example, able to organise and run a saboteur network that can operate across the Schengen area from one Member State or even from across the EU's borders.

Counter-espionage must be made a key element of security work in the EU institutions. The EU's clout in foreign, security and defence policy together with the growing tensions in international relations make EU decision-makers and those who do the preparatory work for them increasingly important targets for hostile intelligence services. With the recently adopted Cybersecurity Regulation for EU institutions, bodies and agencies (EUIBA) and the proposal for a regulation on information security in the EUIBA, the EU has already taken an important step in the right direction. Nevertheless, further emphasis should be placed on strengthening security of equipment and personal devices and making the secure handling of sensitive and classified information across EU institutions, bodies and agencies more efficient. Beyond the respective security systems, facilities and provisions, we need to reinforce a security culture and mindset among EU staff.

Hybrid threats can aim to create distrust fuelling polarisation, as well as **undermining our unity and the credibility of our democratic institutions**. Over the past years, the Commission has already taken steps to counter hybrid threats and enhance democratic resilience across the EU. It adopted the European Democracy Action Plan to build more resilient democracies across the EU by promoting free and fair elections, strengthening media freedom and countering disinformation. With the adoption of the Digital Services Act[11] and its binding obligations for online platforms to combat the spread of disinformation, the Commission also strengthened the Code of Practice on Disinformation. Moreover, the launch of the European Digital Media Observatory and its national hubs increased the capacity to detect, analyse and expose disinformation campaigns.

In addition, the European Media Freedom Act[12] puts in place rules to protect media pluralism and independence, and to shrink the space for disinformation by enhancing media ownership transparency. The Commission also put forward as part of the Defence of Democracy Package a legislative proposal to set up common transparency and accountability standards for interest representation activities seeking to influence the decision-making process in the Union carried out on behalf of third countries. **Work on the upcoming European Democracy Shield envisaged in the Political Guidelines for the next Commission provides a renewed opportunity to outsmart malicious actors by boosting efforts to prevent, detect and respond to disinformation campaigns, and other forms of interference**. Addressing our vulnerabilities, shoring up the resilience of citizens

11. European Commission, Digital Services Act, 2024.

12. European Commission, European Media Freedom Act, 2024.

and institutions and fostering our rapid response abilities are key to protecting our democratic societies [see also chapter 4].

Technological advances highlight and accelerate the evolving nature of methods that can be used against the EU. Disruptive and emerging technologies, such as artificial intelligence provide both new opportunities for building our security, as well as new vulnerabilities from the perspective of all hybrid domains. **Stepping up our technological and economic security in all its facets is an integral part of outsmarting hybrid actors – and the EU should take steps to connect these two policy fields**. We must be able to reap the full potential of technologies for our own security, and at the same time address any security risks they can create. For example, this requires a forward-looking approach to ensure that **emerging technologies**, such as 6G and the Internet of Things, remain compatible with the need for law enforcement authorities to access data for investigations, in accordance with the law, and without undermining cybersecurity or individual freedoms.

In line with its Economic Security Strategy, the EU needs to preserve its capability to service critical infrastructure and maintain economic and cybersecurity, pursuing innovation and technological leadership. This may necessitate reserving participation in EU-funded research, development and innovation projects (RD&I) and their results to EU actors in sensitive areas. The implementation of the recommendation on enhancing research security adopted by the Council in May 2024[13] is an important first step to prevent malicious actors from getting access to sensitive research and knowledge in the EU. The EU and Member States should seize their leading role in standard-setting to build preparedness against emerging threats, to screen foreign direct investment that raises security risks, de-risk undesirable supply chain dependencies, and so on. Moreover, the EU should create cross-silo platforms and tools to safeguard knowledge and innovation by countering intellectual property and technology leakages to malicious actors, especially in sensitive areas (e.g. semiconductors, AI, quantum and biotechnologies). **A shared level of awareness across the EU covering both military and civilian domains, and across the public and the private sectors, is necessary**.

→ Deterrence by punishment

When it comes to the options for response to hybrid activities, there is **a range of measures across the diplomatic, information/intelligence, economic and financial, as well as the legal domain**[14]. The EU has already **substantially upgraded its approach to countering hybrid threats**. This must be accompanied by **better intelligence sharing between Member States and with the EU institutions to** feed into preparedness and decision-making. Actionable intelligence is essential to enable legislative action, effective strategic communication, as well as readiness to use tools, such as sanctions, protective full-scale cyber operations and information campaigns to counter disinformation.

Deterrence by punishment should be built on finding with increasing accuracy the best ways to target the threat actor with consequences. This requires an advanced understanding on 1) what different hybrid actors value the most and what their weak spots are, and 2) what their cost-benefit calculus for conducting particular hybrid operations is. In the EU, we still lack a consistent and shared analysis of the vulnerabilities and dependencies of our adversaries. This is necessary to identify the most effective options to deter, discourage and respond to those adversaries. In the modern interconnected global economy, most hybrid actors benefit from interaction with the EU in some way, which gives us leverage. Member States and the EU have a wide range of options, but not all the tools have the same impact on all actors. **The EU must follow and analyse better the impact of each tool in each case, and learn to use them more effectively in every context**. As the effects and responses are by design cross-sectoral, the tools should be assessed

13. Council of the European Union, Council Recommendation on enhancing research security (C/2024/3510), 2024.

14. The Hague Centre for Strategic Studies, Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework, 2023.

and deployed utilising analyses and forecasts of their cascading effects for the EU, the perpetrator, and any possible third parties concerned.

A more nuanced understanding of different threat actors and their aims and vulnerabilities is necessary, also in the context of attribution. Many actors give a high priority to preventing the detection of their activities, or at least maintaining plausible deniability. Some others see benefits in making their operations detectable and even known publicly (while not overtly admitting their responsibility) to raise concerns and fear with the intention of showing off their own strength and highlighting the target's vulnerability. Revealing the actors behind hybrid operations publicly may also help to raise the awareness of citizens on certain tactics that may be used also directly against them, for example in the media and information sphere. **'Naming and shaming' are among the diplomatic measures to be further expanded**.

Key to changing the cost-benefit analysis of threat actors is to **make the EU not only stronger in its ability to respond, but also more difficult to predict**. This calls for a smarter decision-making culture in the EU. The EU needs to increase the **strategic ambiguity** of its deterrence by extending its response options as widely as possible, and not ruling out any options in advance. Reducing the number of advance leaks to the press, which can undermine decision-making processes at sensitive moments and erode unity, will be an important aspect in this regard. Furthermore, ensuring faster and – most importantly – stronger decisions, for example on restrictive measures, will also be essential to reinforcing the credibility of the EU's readiness to respond. Also here, outsmarting works both ways. We need to realise that hybrid actors try to maximise their deterrence based on ambiguous red lines against us, as well as information manipulation, including bluffing.

The EU does not and cannot respond to hybrid campaigns in ways that would not be in full compliance with national, EU and international law, as well as our European values. In addition, an in-kind or symmetric response to hybrid operations, which are designed to target the vulnerabilities of our open and democratic societies, may not always be as effective against our adversaries. **This is why in most cases an asymmetric response may be more effective and play to the EU's strengths. In particular, we can use asymmetry to our advantage to increase the ambiguity of our response**. For instance, without framing them expressly as counter-hybrid operations, the EU and Member States can use legal proceedings (e.g. anti-corruption, tax evasion measures, environmental inspections at sea, anti-coercion etc.), as well as actions in other domains, such as trade (e.g. anti-subsidy or anti-dumping investigations, leading to access restrictions to the Single Market) to raise the costs for threat actors.

In short, the EU should clearly signal to hybrid threat actors that they will no longer be able to escape consequences for their damaging activities. In the best case, **a well-prepared EU would be more able than it is today to prevent many hybrid threats from materialising in the first place by undoing the plans of malicious actors**. Preparing to be able to carry out a coherent and united response in itself undermines the very objectives behind hybrid operations that aim to increase divisions within the EU and paralyse our ability to respond. In doing so, we can show **threat actors that openness, democratic scrutiny, pluralistic media and the rule of law are strong assets that we can use to our advantage against their malicious intents**.

Cooperate with partners to narrow the space for hybrid threat actors

Finally, close cooperation with the EU's partners in this context should aim to strengthen our deterrence through broader response (for example, shared attribution, coordinated sanctions, and other measures), and reduce the risk of retaliation. In this regard, the President's Political Guidelines for the next mandate already envisage an expansion of the Cyber Diplomacy Toolbox and reflections on a dedicated sanctions regime for hybrid threats.

Sharing and learning lessons with and from partners who are targeted by high-intensity hybrid operations is another important work strand. Together with partners such as the US, the UK, Japan, Australia, and Canada, but also Ukraine, Taiwan, and many others, we can build mutual resilience and together reinforce our preparedness and awareness to the heightened hybrid threat levels arising from the deteriorating geopolitical context. By jointly investing in raising global awareness on hybrid threats, we can clearly communicate how hybrid activities undermine stability and trust globally – causing damage also beyond the EU – and increase pressure on persistent threat actors [see also chapter 8].

Recommendations

1. **Strengthen EU intelligence structures by working step-by-step towards a fully-fledged EU service for intelligence cooperation.**

2. **Reinforce the EU's capacity for deterrence by denial:**
   - × Take joint action to make it as difficult as possible for hostile intelligence services to operate within the EU.
   - × Encourage Member States to proactively share information about vulnerabilities that pose a broader threat within the Union and should be tackled together at the EU level.
   - × Establish an anti-sabotage network to support Member States in preventing and responding to sabotage incidents.
   - × Strengthen the links between the work on countering hybrid threats and the promotion of economic security.
   - × Ensure effective support to Member States facing instrumentalised migration at the Union's external borders.

3. **Reinforce the EU's capacity for deterrence by punishment:**
   - × Provide an up-to-date and a comprehensive assessment of key hybrid threat actors' strategic and operational specificities to identify aims and methods, as well as key vulnerabilities and exposure to EU countermeasures.
   - × Reinforce political attribution as the basis for response to hybrid threats and consider on a case-by-case basis the public use of (declassified) intelligence assessments.
   - × Ensure the creation of a robust framework for lawful access to encrypted data — while respecting fundamental rights — to support the fight of Member States' law enforcement and security authorities against espionage, sabotage and terrorism, as well as organised crime.

1. STRENGTHEN EU INTELLIGENCE STRUCTURES STEP-BY-STEP TOWARDS A FULLY-FLEDGED EU SERVICE FOR INTELLIGENCE COOPERATION

All security actors need reliable and timely intelligence on the threats they face to guide both political and operational decision-making. As outlined above, deterrence by both denial and punishment fundamentally relies on our ability to better understand different threat actors' behaviour, their tactics, and concrete aims. In this sense, the first step of outsmarting malicious actors is to know as accurately as possible how 'smart' they are in working against us.

To ensure the EU's capacity to take autonomous and decisive action in the face of elevated threat levels, there is an urgent need to take better advantage of intelligence analysis at the EU level. Decision-makers in the EU institutions and Member States need to have a clear and timely understanding of threats and clandestine activities targeting the Union. This is why reinforcing the EU's Single Intelligence Analysis Capacity (SIAC), consisting of the EU Intelligence and Situation Centre (INTCEN) and EU military intelligence as part of the EU Military Staff in the EEAS (both working under the High Representative) is a core priority, as recognised in the Strategic Compass. SIAC already provides strategic analysis based on intelligence shared by Member States, supported by open-source intelligence (OSINT).

A number of challenges still need to be addressed.

- First, the intelligence sharing from Member States on which SIAC relies needs to be further strengthened and structured, including to target concrete operational needs at the EU level. The aim is also to make sure that EU leaders have available the best possible intelligence to guide informed decision-making both on long-term strategic needs, as well as in a crisis demanding urgent action, and that the policies of relevant services are based on robust intelligence threat assessments.

- Second, the links between external and internal security should be better reflected in our intelligence structures, including through enhanced interinstitutional information sharing for operational needs, for instance with services in the Commission that deal with various dimensions of security and manage and support relevant networks. Such cooperation between SIAC, Commission services and also EU Agencies (such as Europol, Frontex and ENISA) exists today, but lacks formal structure to be fully exploited both at the operational level and to inform strategic policy-making and crisis response.

- Third, in most sectors, Member States and European partners cooperate and share intelligence informally through different formats. This cooperation serves clear purposes and brings added value to European cooperation between intelligence organisations, but its informal nature and lack of EU legal basis mean that it cannot directly support EU decision-making or provide day-to-day, 24/7 support to the Union's activities.

As a long-term objective, the EU should have a fully-fledged intelligence cooperation service, serving all EU institutions and Member States. The goal should not be to emulate the tasks of Member States' national foreign intelligence and domestic security services, nor to interfere with their prerogative on national security. Instead, focus should be on further developing SIAC into a service that can fully support the EU's activities and institutional leadership in line with the Union's broad and unique role as a security provider in respect of and in complementarity with the Member States' national capabilities in intelligence gathering. This should also support the counter-intelligence work of the EU institutions in protecting themselves, their information systems and their staff from clandestine activities.

Moreover, strengthening intelligence cooperation at the EU level should be done by establishing stronger frameworks for regular and structured intelligence sharing across policy domains – in full complementarity with and respecting Member States' prerogatives in terms of intelligence gathering. This could better support the operational and policy planning needs of the relevant EU institutions and agencies, joint ad hoc or forecasting projects, the research and innovation efforts of Member States' services, and issuing timely and coordinated 'crisis warnings' to private sector representatives.

Concrete steps forward would include:

- Implementing the steps agreed by the Council as part of the implementation of the Strategic Compass to reinforce and improve SIAC, including the Hybrid Fusion Cell, also with a view to strengthen its role in support of political decision-making within the Council in the context of hybrid and wider security and defence matters. This may include further strengthening SIAC with staff and with specific data analysis and language skills to meet the increasing demands posed by the EU's deteriorating security environment.

- Ensuring a structured and coordinated process to address information requirements and requests for SIAC products in a timely manner, including from relevant Commission services and the EU agencies under their oversight.

- Strengthening and formalising information and data-sharing arrangements between SIAC and other relevant EU-level actors, such as the EU Satellite Centre (SATCEN), Europol, CERT-EU, the Commission's new Cyber Situation and Analysis Centre, and the EU's network of delegations

abroad with a view to better aggregating information that not only supports short-term actions and response measures, but also feeds into long-term policy planning in the context of preparedness.

- Enhancing cooperation between SIAC and relevant security departments/units of the Commission, the EEAS, the General Secretariat of the Council, as well as other EU institutions and Member States to coordinate specific counter-espionage tasks, strengthen the security and counter-intelligence culture in the EU institutions, and further develop their ability to counter threats against them posed by hostile foreign intelligence services.

- Developing a proposal together with the Member States on the modalities of a fully-fledged intelligence cooperation service at the EU level that closes the remaining gaps and better connects internal and external security with fast and accurate intelligence assessments that can serve both strategic and operational needs of EU-level policy-planning and decision-making.

2. REINFORCE THE EU'S CAPACITY FOR DETERRENCE BY DENIAL

→ Take joint action to make it as difficult as possible for hostile intelligence services to operate within the EU

Discrepancies in Member States' counter-intelligence practices, legislation and insufficient cross-border information sharing can be exploited by malicious actors. While these matters concern national security and are therefore the competence of each Member State, EU-level cooperation could help to minimise the threats we face from foreign intelligence services who aim to do harm against us. To ensure that no Member State can be abused as a safe haven or a weak link for foreign intelligence services to operate against other Member States, the EU institutions or any other international organisations located within the EU, Member States should:

- Align and harmonise minimal legal definitions and measures across the Member States to criminalise all espionage and related illegal clandestine activities.

- Ensure smooth information sharing between competent national authorities when representatives of hostile intelligence services are expelled from one Member State to prevent their redeployment to another Member State at a later point (even under a new alias). For instance, this could include a common secure database of high-risk individuals.

- Set restrictions, when necessary, on the freedom of travel of diplomatic personnel and citizens of a country posing a threat to the EU through sabotage, espionage and similar activities. It should be taken into consideration that expulsions and any restrictions will most likely be met with similar measures against EU diplomatic staff and citizens by the country in question.

→ Encourage Member States to proactively share information about vulnerabilities that pose a broader threat within the Union and should be tackled together at the EU level:

Given our interdependencies, vulnerabilities in individual Member States, such as insufficiently protected IT systems, economic dependencies or domestic actors that are used as proxies by third countries can cause serious spillovers across the Union. If Member States do not warn each other in advance, we may find ourselves on the backfoot as we react to the next 'high impact-low probability' incident. This is why promoting a culture of proactive information sharing on vulnerabilities is essential to step up collective preparedness and to rigorously address vulnerabilities together. In this regard, the EU should further build on cybersecurity vulnerability disclosure requirements under the NIS2 Directive, extending, where appropriate similar practices to other sectors.

Given the sensitivity of exposing vulnerabilities, proactive information sharing needs to be based on a) secure and autonomous information-sharing and communication systems [see chapter 3, recommendation 3] and even more importantly, trust. Trust needs to be built over time. As suggested in

chapter 3, we may want to start by building 'variable geometries' of information sharing, bringing together coalitions of willing Member States that are ready to be transparent about their vulnerabilities with each other.

→ Establish an anti-sabotage network to support Member States in preventing and responding to sabotage incidents:

Considering the recent increase in sabotage incidents and attempts across Europe, the EU and Member States should strengthen operational cooperation in preventing and investigating sabotage by malicious actors and their proxies. Building on first steps in the context of the EU Critical Infrastructure Blueprint, a dedicated anti-sabotage network at the EU level bringing together experts from Member States' competent authorities could provide assistance to any Member State dealing with a sabotage-related threat or emergency. Upon request, the network could be activated to launch a targeted operation (limited in time and scope). Such a network could build upon existing EU-level cooperation, notably the Critical Entities Resilience Group, the Protective Security Advisory Programme, the work of the INTCEN Hybrid Fusion Cell, as well as the cooperation of Member States' intelligence/security services, law-enforcement[15], border and coast guards (including Frontex), customs, and other competent authorities. Deployments could focus on both prevention and preparedness, for example by sharing best practices on protecting critical infrastructure from sabotage, 'sabotage resilience stress-tests' or additional personnel, to help protect objects under a particularly serious threat, as well as response aspects – for instance, by providing support to investigations and damage control operations. In the long term, the network could become part of a strengthened mandate for Europol.

→ Strengthen the links between the work on countering hybrid threats and the promotion of economic security.

As the connection between economy and security is ever stronger in the contested international environment, there is an urgent need to connect the work on countering hybrid threats to efforts aiming to promote the EU's economic security. Supply chain dependencies, future digital infrastructure, foreign direct investment, research security, and new clean technologies are leveraged by competing and malicious global powers to create the potential for weaponisation and build up leverage to be used as part of coercive strategies – alongside data gathering and the harvesting of technologies for civilian-military fusion. Addressing vulnerabilities and gaps in our resilience in these areas will diminish the surface areas for future hybrid attacks, while also staying attentive to the evolving tactics of hybrid actors. Further efforts to implement the EU's Economic Security Strategy should take into account the evolution of the EU's counter hybrid policies – and vice versa.

→ Ensure effective support to Member States facing instrumentalised migration at the Union's external borders.

There is an urgent need to further support Member States along the EU's external borders who face well-planned hybrid operations by malicious State actors, exploiting human beings and cynically trying to weaponise EU' core values to undermine the EU's security. To this end, the EU and its Member States should explore further ways to support the exposed Member States, including notably in the context of the new European Migration and Asylum Strategy announced in the Political Guidelines of the European Commission's President for the next mandate.

15. For instance. the ATLAS network of Member States' law enforcement intervention units.

In exceptional crisis situations affecting the security of the Member States and the Union, assessing the right balance between the right to asylum, other migration aspects and essential security interests is necessary. The strengthening of Frontex, as already proposed by President von der Leyen, is of key importance to ensure it can support Member States in protecting our common borders in all circumstances with strong governance and the full respect for fundamental rights. The possible use of the Integrated Border Management Fund to support investments in infrastructure, equipment and systems could be explored.

3. REINFORCE THE EU'S CAPACITY FOR DETERRENCE BY PUNISHMENT

→ **Provide an up-to-date and comprehensive assessment of key hybrid threat actors' strategic and operational specificities to identify aims and methods, as well as key vulnerabilities and exposure to EU countermeasures.**

In doing so, the EU can identify the most efficient tools and legal instruments to deter, discourage and respond to specific adversaries by creating the highest possible deterrent within a fully coordinated and proportionate response. Building on this assessment of hybrid threat actors, we should then identify, organise and grade all tools at our disposal in an actor-specific way to enhance our capacity to act coherently and efficiently. Experience shows that restrictive measures usually do not lead to an immediate change in behaviour, but they need to be seen in this context as a tool to alter the cost-benefit analysis of the targeted actors over time by making it as difficult, slow and costly as possible for them to carry out the malicious activities that have led to the imposition of sanctions in the first place. Here, we need to take into account that threat actors are actively building up their resilience to international sanctions, including through alternative structures, buffers and supply chains, and they are actively learning from each other how best to evade sanctions. To maximise the impact of sanctions and minimise the ability of sanctioned actors to evade them, we should take full advantage of the excellent work of EU Sanctions Envoy David O'Sullivan over the past years.

→ **Reinforce political attribution as the basis for response to hybrid threats and consider on a case-by-case basis the public use of (declassified) intelligence assessments.**

In line with a 'naming and shaming' logic, the EU and Member States should promote rapid **political attribution** as the basis for response to hybrid threats. Rapid attribution can be an effective way to seize the initiative and place hybrid actors on the backfoot. While its effectiveness as a deterrent may vary, some malicious actors may be particularly susceptible to the reputational damages linked with rapid and decisive political attribution. While attribution is usually a lengthy and complex process burdened with considerable uncertainty, the EU and Member States should keep in mind that the State actor suspected of hybrid action against the EU will not have a genuine interest to cooperate in any technical investigation concerning the matter and will instead likely aim to distort its meaningful outcome. This cannot prevent the EU from making a political attribution trusting its own information and taking the necessary action. Furthermore, faster political attribution could also provide a basis for making better use of Europe's sanctions toolbox.

The EU and Member States should also consider on a case-by-case basis the coordinated public use of (declassified) intelligence assessments to prevent or disrupt malicious plans of foreign actors or to respond to and deal with the consequences of hybrid operations. For instance, the public use of intelligence could be instrumental in shoring up public opinion in certain situations, and in this way prepare for or prevent malicious activity. This includes the possibility to actively provide information to the public on evolving situations, where appropriate, not to allow malicious third countries to set the narrative.

→ **Ensure the creation of a robust framework for lawful access to encrypted data — while respecting fundamental rights — to support the fight of Member States' law enforcement and security authorities against espionage, sabotage and terrorism, as well as organised crime.**

In this context, EU and national authorities need to expand and improve the capacity to investigate hostile and criminal activities in the digital domain, fully respecting fundamental rights, without undermining cybersecurity. Law enforcement authorities across the EU have in practice lost access to the relevant electronic evidence. More and more communications are now taking place through service providers based in other jurisdictions. Finally, most of those communications are now end-to-end encrypted, so that even if telecommunications providers cooperate with law enforcement authorities, data provided would not be useful. Cooperation with providers based in other jurisdictions would be required to obtain the necessary access to data. There is a clear nexus between organised crime and threats to national security, as terrorist groups engage in organised crime, among other activities, to finance their activities and recruit members. There are signs that in several recent cases of sabotage that have been executed or attempted against EU Member States, perpetrators were recruited and instructed via digital communication applications. The ability to lawfully access encrypted data is important to counter such threats, as well as for the fight against terrorism and organised crime. Addressing this challenge requires a forward-looking approach taking into account the evolution of technologies, such as 6G and the Internet of Things.

CHAPTER · CHAPTER · CHAPTER

07

Scaling up Europe's defence efforts and unlocking its dual-use potential

Europe's monumental task

Stronger European defence – based on a competitive and resilient European defence technological and industrial base and strengthened defence capabilities and readiness – is of crucial importance for the EU's comprehensive preparedness. Shoring up the ability of Europeans to defend themselves in a volatile and dangerous world provides an essential public good that underpins the well-being of the EU's citizens, while creating a safe environment for the Single Market[01]. Security and defence are at the heart of the European project, as the President of the European Commission has declared on various occasions[02].

The challenges the EU faces in this regard are monumental. Europe's strategic context has fundamentally changed with Russia's full-scale assault on Ukraine. Its defence capability, industrial and technological gaps are still wide, however, and in some areas are growing further. The EU's fragmented capability landscape and shallow production lines reflect long-standing nationally oriented defence

01. See, for example: Fondation Robert Schuman, The Sword and the Marketplace: Europe Needs a Defence Union to Support its Economic Integration, 2018.

02. European Commission, Keynote speech by President von der Leyen at the EDA Annual Conference 2023: Powering up European Defence, 2023.

industrial policies[03]. **Yet, the EU's drive to fix these gaps most urgently through collective action seems to be faltering**.

Europe's armed forces need to urgently prepare for the full spectrum of military and civilian-military contingencies, including the elevated risk of external armed aggression. Such scenarios need to incorporate the likelihood of a further US pivot to East Asia in the allocation of forces, spare parts and munitions, but also the design of new capabilities. The US expects European allies to provide at least half the forces necessary for the defence of the Euro-Atlantic area[04]. Currently, the collective inventory of the capabilities of Member States (most of which are also NATO allies) continues to show serious gaps and shortfalls, including long-standing dependencies on the US, especially in high-intensity operations[05]. As identified in recent experiences and reflected in capability planning processes, the EU-27 are lacking in nearly everything from ammunition and strategic enablers to high-end capabilities[06]. Prominent American analysts have warned that Europe's strategic dependency on the US has only grown, not diminished, since 2022[07]. **This leads to critical questions of how Europe can shore up its defences – and do it at a much faster pace than it has so far – and in a joined-up manner**.

Sticking to predominantly national approaches, as is currently largely the case, will not be sufficient. Currently, Europe is outpaced by the US in the innovation-heavy air domain [see Box 13 on drones below] and 'out-massed' by the Russians in significant categories in the land domain[08]. South Korea has recently manifested itself as a competitive defence supplier for Europe. Chinese defence companies now rank among the largest in the world[09].

Overall, Europe needs to hedge its bets. Delivering high-tech capabilities plays into our comparative technological advantage, considering the global race for technological dominance. At the same time, we need to build up sufficient mass in case any military confrontation turns to longer term attrition. The EU therefore needs to strengthen its industrial capacity to **develop and produce cutting-edge capabilities more efficiently and much faster, while scaling up the production of ammunition and other basic materials** that is needed in war in significant quantities, can be used without multi-year training, and moved quickly from production lines to the battlefield. It is necessary to draw lessons from Ukraine's experience during the war and of our ongoing support to Ukraine to find the best practical solutions to make this happen.

Moreover, European defence should be more than about military hardware and defence industrial and technological capacity. Europe' defensive capacity hinges on a whole-of-government approach to preparing for major (military) crises. Member States' armed forces can benefit from being better connected to other crisis actors and critical sectors through enhanced civil-military cooperation and dual-use technologies and infrastructures. Only this way can Europe build up the whole-of-government preparedness and societal resilience that will be vital if a major military crisis erupts [see chapter 2].

03. Estimates are that Europe operates 5 to 6 times more military systems than the US – 179 versus 33 systems in 2023 (McKinsey, based on the Military Balance). Fragmentation is uneven per sector, while displaying less fragmentation in some segments (e.g. in the naval domain) than in other areas (such as, main battle tanks), especially when discounting legacy equipment. Europe also has roughly 1.5 times more production lines for key capabilities than the US, but within a much smaller market – 41 versus 25 in the EU and US respectively. Based on EUISS, Building weapons together (or not): How to strengthen the European defence industry, policy brief 20, 2023.

04. See: International Institute for Strategic Studies (ISS), The Future of NATO's European Land Forces: Plans, Challenges, Prospects, 2023.

05. See, for example, the in-depth analysis: Centre for Strategic and International Studies (CSIS), Europe's Missing Piece: The Case for Air Domain Enablers, 2023.

06. The EU's 2023 Capability Development Plan sets out 22 overarching priorities across all capability domains.

07. See: Brookings Institution, Strategic responsibility: Rebalancing European and trans-Atlantic defense, 2022.

08. See, for example: Wolff, G.B., Burilkov, A., Bushnell, K., and Kharitonov, I., Fit for war in decades: Europe's and Germany's slow rearmament vis-à-vis Russia, Kiel Report 1, Kiel Institute for World Economy, 2024.

09. Three out of the ten largest defence companies in the world are now Chinese. See: Defense News, Top 100 for 2024, 2024.

Member States' armed forces also play an important role in assisting other governmental actors in their domestic tasks. They support search and rescue, large-scale evacuations, and response to disasters, depending on national constitutional arrangements. They have often been called upon to support civilian authorities in the context of the COVID-19 pandemic (e.g. to provide back-up transportation or medical facilities, or to ensure a security presence) and in disasters (e.g. heavy lifting capacities).

While recognising NATO's primary role in the collective defence and deterrence of its members, the EU brings particular strengths in the context of preparedness and readiness, given its broad policy range as well as ITS regulatory/legislative and financial powers. Based on the Single Set of Forces principle, a coherent set of priorities and using NATO military standards wherever available, the EU's support for Member States' defence needs entails joint defence research and development, aggregating demand, harmonising requirements, strengthening the supply chain and production capacity of the defence sector and facilitating joint defence procurement. The EU is well placed to further strengthen and rationalise Europe's defence readiness, as part of its comprehensive preparedness drive. **It contributes to a stronger and more European NATO**.

The White Paper on the future of European Defence, envisaged in the Political Guidelines (2024-2029), offers an opportunity to discuss with the Council and European Parliament, the public and other stakeholders, what the short, medium and long-term ambitions and policies should be. This ambition should be to arrive at a coherent, credible and connected full spectrum package of European defence capabilities, based on ramped-up defence industrial production capacity and accelerated defence technological innovation cycles. The aim should be to be ready the Union – in close cooperation and complementarity with NATO – for **the demands posed by the need to deter an all-out war fought across land, sea, air, space and cyber space that may last years**. This poses a whole different set and scale of demands for our armed forces, economies and societies. It provides a challenging starting point to develop a genuine whole-of-government approach to the defence readiness of Europe. **The stronger defence readiness of EU Member States is necessary both for deterring Russia, as well as to support Ukraine in a way that makes a just peace possible, and prevents further Russian aggression**.

All this in turn requires increasing and optimising the use of available financial resources. Given that national defence budgets are already growing, it would be a missed opportunity of historic proportions if Member States fail to coordinate and rationalise their defence expenditures. Precisely now, we should avoid past mistakes and unlearn bad habits: uncoordinated and disjointed spending at the national and EU levels, often fragmented along national lines –sometimes competing for limited supplies – and compartmentalised along sectorial lines (with firewalls between defence and civilian expenditures, etc). Short-term decisions, driven by a sense of urgency, have long-term implications on the structure of European defence.

Reality check

There have already been many initiatives to enhance the level of coordination and collaboration in European defence. After the wave of EU defence initiatives in 2016-2020, including the launch of the Permanent Structured Cooperation and the European Defence Fund, new steps were taken in the wake of the Russian aggression against Ukraine through the Strategic Compass for Security and Defence (March 2022) and the Defence Investment Gaps Analysis (May 2022). Building on the initial success of the European Defence Fund, new innovative funding instruments were developed for joint procurement (EDIRPA) and industrial ramp-up (ASAP)[10]. Moreover, the European Defence Industrial Strategy (EDIS) of March 2024 has put forward concrete proposals to increase the EU's defence read-

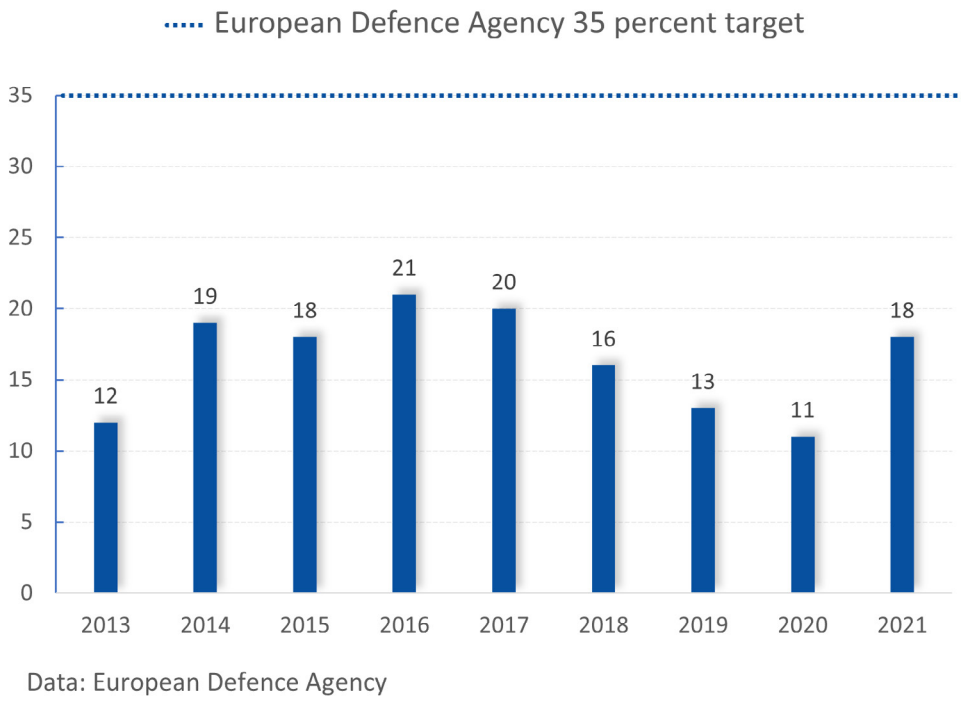
10. EDIRPA: Regulation (EU) 2023/2418 on establishing an instrument for the reinforcement of the European defence industry through common procurement; ASAP: Regulation (EU) 2023/1525 on supporting ammunition production.

iness. It was backed up by the proposed European Defence Industrial Programme (EDIP) Regulation that is currently under discussion in the Council and the European Parliament.

Yet, according to the latest available figures, Member States are still far from achieving the benchmark they set for themselves over 15 years ago in the EDA – as replicated as a commitment in PESCO – to invest 35% together on European collaborative projects [see Figure 9]. This is a prerequisite to able to progress towards the even higher benchmark proposed in the EDIS[11]. Overall, the current funding levels of EU defence instruments incentivising cooperation remain relatively limited compared to the overall defence investments of Member States. This limits its effect on the market. The political priorities set out by President von der Leyen in her Political Guidelines (2024-2029) propose to further reinforce the European Defence Fund (EDF) and the European Defence Industry Programme (EDIP).

FIGURE 9

Share of collaborative defence equipment spending (2013-2023) and the EDA's 35% target



Source: Based on Munich Security Conference as well as data from the European Defence Agency, 2024.

More importantly, however, the overall political momentum and drive from the side of Member States seems to be – paradoxically – less than it was some years ago, even if the security situation has further worsened since then. EU citizens' expectations are meanwhile clear. In a recent Eurobarometer, 80% of respondents across the Union felt that EU-level cooperation on defence matters should increase and two-thirds agreed that the EU should spend more money on defence[12]. As defence spending increases, we should pay all the more attention to how the money spent strengthens our defence readiness most efficiently and ensure that it produces the capabilities that are most needed.

11. In 2021, 18% of their equipment budgets was spent on European collaborative projects. The benchmark of spending 35% of Member States' total equipment budget on European collaborative equipment procurement was established by Defence Ministers in the EDA Steering Board in 2007. It was replicated as part of the more binding commitments in the framework of the Permanent Structured Cooperation. EDIS now proposes, in order to shift towards a sustained, long-term demand signal to the EDTIB, to achieve the goal of procuring at least 40% of defence equipment collaboratively by 2030.

12. European Commission, Standard Eurobarometer 101 - Spring 2024, 2024.

Despite major steps forward thanks to different initiatives over the past 20 years, it has proven very difficult to truly rationalise and reform European defence. The reasons for this vary and differ for each Member State, ranging from political trust to diverging financing, industrial and institutional preferences. Multinational defence cooperation **offers the potential for cost savings**, due to economies of scale not only in the acquisition phase, but throughout the life cycle of equipment[13]. Moreover, some capabilities have become simply too expensive to develop on a strictly national basis, even for the largest Member States. But collaborative projects do **require an additional effort from national institutions**, while introducing certain risks and complexities. Impediments to cooperation range from difficulties in **harmonising requirements** due to differing strategic and military doctrines, the misalignment of **available financing**, agreement on **equitable industrial shares**, the involvement of more industrial entities and **complex supply chains**, and ultimately a l**ack of political will and trust**.

Europe's fragmented defence market is composed of a **small number of Member States with sizeable defence industries**, with different types of intra-EU or extra-EU ownership structures, although the supply networks of the 'primes' (i.e. defence companies that produce major military platforms) do extend across Europe[14]. It is moreover a **heavily regulated sector**, due to specific requirements for permitting and licensing even within the Single Market. Efforts to introduce a greater **market-driven approach** in the defence sector through the 2009 defence procurement directive have not led to significant improvements given the major exemptions allowed to Member States in case of national essential security interests or government-to-government sales (which applies mostly to the US).

There is therefore still a lot of scope to **incentivise, facilitate and simplify cooperation and consolidation in the EU's defence sector. A Single Market for Defence Products and Services** as called for by the European Council and envisaged in President von der Leyen's Political Guidelines (2024-2029) may constitute an important step forward. This cuts across an intractable issue with deep roots in the history of European integration[15]. The report on the future of European competitiveness by Special Adviser Mario Draghi offers further analysis and suggested remedies in this regard.

At the moment, however, there is a real risk of going in the opposite direction and of the further fragmentation of European defence. The level of joint and collaborative investment is not keeping pace with fast-growing national defence budgets, as current data suggests[16]. This would contradict the policy goals of the relevant frameworks and instruments – such as PESCO – that Member States have put in place in the past years. It also contradicts the overall analysis, shared across Member States, that the deteriorating strategic context calls for an urgent effort to close joint investment, capability and technology gaps.

Adequate funding is a vital precondition for building credible defence preparedness and readiness for the EU and its Member States. As part of its call to explore all options for mobilising funding, the European Council asked in June 2024 for developed options for public and private funding to strengthen the defence technological and industrial base and address critical capability gaps. Such options are urgently required to bridge the budgetary and investment gaps at the EU level [see also chapter 9], including in view of the next MFF.

13. McKinsey has projected that a theoretical scaling-up of European defence industrial programmes to US levels could allow for cost efficiency gains of around 30% (17% for labour costs and 14% for material). However, this would assume that requirements are kept under control. See: McKinsey, The future of European defence: Tackling the productivity challenge, 2013.

14. Centre for Security, Diplomacy and Strategy (CSDS), Beyond fragmentation? Mapping the European defence industry in an era of strategic flux, CSDS In-depth 7, 2023.

15. See: CEFISO, Markets in Defense of Europe: Providing Public Goods in European Defense, EconPol Forum 4, Volume 25, 2024.

16. For 2024, NATO predicts an increase of defence expenditures for NATO Europe and Canada by 17.9%. See: NATO, Defence Expenditure of NATO Countries (2014-2024), 2024.

A preparedness approach to the defence of Europe

The strategic, military, economic and political case for more powerful and less fragmented European defence has been made time and again. The EU provides a unique platform to bring national efforts and resources together to **unlock economies of scale, avoid fragmented and inefficient spending, and ensure interoperability. It is now time to focus on concrete action at a much higher level of ambition and scale, applying a preparedness and readiness logic to our efforts**. After all, Europe's ability to defend itself or to conduct operations at the highest levels of scale and intensity is impaired by long-standing gaps, shortfalls, and external dependencies that we can only fix through an effective, long-term joint strategy.

The relative lack of European defence cooperation remains a hindrance for stronger military readiness.

- Europe's endemic fragmentation along national supply and demand lines in the defence sector has **weakened the competitiveness of the European Defence Industrial and Technological Base** (EDTIB)[17]. Apart from a predominantly national focus, with over 80% of national defence investment spent in respective national industries, Member States also often procure from outside the EU – notably in the US (especially in the air domain) and more recently in South Korea[18]. The European assembly lines for the F-35 and Patriot missile systems do generate local and European economic benefits, but also crowd out fully-fledged European alternatives. Apart from export control restrictions (which have come to the fore when discussing the possible transfer of US or German produced capabilities to Ukraine, for example), this has in turn **created security of supply dependencies which may be exposed in a multi-front scenario, as experts have warned**[19].

- **The patchwork of national defence forces operating different types of equipment creates vulnerabilities in the event of a major military contingency**, notably related to interoperability/inter-changeability resulting from the differentiated supply and production lines for spare parts, munition, repairs, etc. All this is on display in Ukraine at the moment, which is operating different types of equipment from European countries. Using the same equipment creates opportunities for scale and collaboration throughout the lifecycle of that equipment and in all dimensions of the capability process (from training and doctrine to munitions, maintenance and repairs) – as long as rigorous standardisation is pursued throughout (i.e. avoiding the proliferation of national configurations and industrial variations).

Decades of underinvestment in defence by most EU Member States has weakened the operational readiness and pace of innovation of their armed forces.

- The stocks and inventories that are needed in a prolonged conflict have dwindled significantly over time [see Figure 10]. They were often the first categories to be cut back during the period of defence budgetary contraction following the end of the Cold War. European assistance to Ukraine has shown the same lack of sizeable stocks and production capacity for artillery ammunition and

17. In February 2024, McKinsey assessed that there were two to three times as many European suppliers competing at the platform level (aircraft, tanks, and ships) compared to the US. On average in 2021, before the recent turn in defence posture, Europe's leading defence companies had 30% of the revenues of an average US defence company and operating margins were lower by around two to three percentage points. See: McKinsey, Innovation and efficiency: Increasing Europe's defense capabilities, 2024.

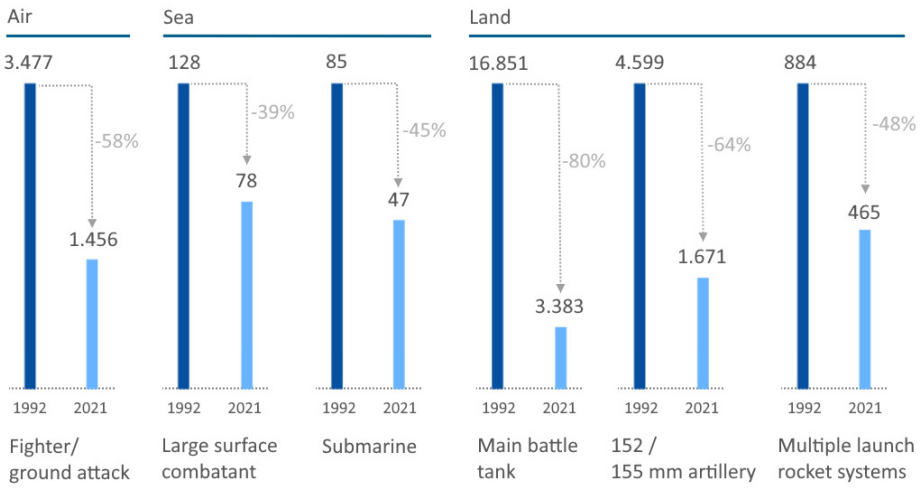
18. In March 2024, SIPRI reported that States in Europe almost doubled their imports of major arms (an increase of 94%) between 2014 and 2018, and 2019 and 2023. Around 55% of these imports from 2019 to 2023 were supplied by the US, up from 35% in 2014 to 2018. See: SIPRI, European arms imports nearly double, US and French exports rise, and Russian exports fall sharply, 2024.

19. RUSI, Regenerating Warfighting Credibility for European NATO Air Forces, 2023. RUSI, Europe Must Urgently Prepare to Deter Russia Without Large-Scale US Support, 2023.

missiles in particular, which will take years to rebuild. The needed size of European stocks must be measured against Russia's production capacity, which has been increasing since 2022 faster than rearmament in the West, as has been illustrated for example by the recent comparison by the Kiel Institute[20].

FIGURE 10

Reductions in selected EU countries' inventories in selected equipment categories prior to Russia's invasion of Ukraine (1992-2021)



Source: Based on Munich Security Conference as well as data from IISS, 2024.

- The underinvestment in defence across Europe since the end of the Cold War has led to a **decrease in the volume of major military platforms**. Comparing 2022 to 1992, the inventory of main battle tanks fell by 77%, fighter jets by 57%, large surface combatants by 39%, and submarines by 47%. Current platforms have an enhanced capability compared to those of a generation ago, but it is nonetheless necessary to rapidly **increase the depth and breadth of Europe's armed forces**. Given the time lag of modern industrial production – it reportedly takes up to two years to produce a main battle tank – this will take years, if not decades to achieve.

- **The remaining military capabilities in Europe often suffer from a lack of operational readiness**, as the necessary supporting capacities and logistics were cut back under budgetary constraints. NATO figures in this regard are classified, but older studies dating back to 2015-2016 –the height of the Afghanistan operations – indicate that around 30% of Member States' land forces were 'deployable' while only 6% of the total could be sustained in operations at any given time (due to rotations, logistical constraints, etc.) – and perhaps even lower than that[21]. Against the backdrop of NATO's 50% deployability benchmark and its New Force Model, the Alliance has devoted several major initiatives to strengthening the military readiness of its (European) allies. In particular strategic enablers, such as logistics and ISR capabilities, are often lacking, despite positive steps forward in recent years. For example, in medium and heavy UAV's(56 versus 297), Europe is relatively undersized compared to the US. The same applies to transport aircraft (210 versus 488) and tanker aircraft (26 versus 408)[22].

20. Wolff, G.B., Burilkov, A., Bushnell, K., and Kharitonov, I., Fit for war in decades: Europe's and Germany's slow rearmament vis-à-vis Russia, Kiel Report 1, Kiel Institute for World Economy, 2024.

21. McKinsey, More tooth, less tail: Getting beyond NATO's 2 percent rule, 2017.

22. See: Grand, C., Defending Europe with less America, Policy Brief, ECFR, 2024.

In the logic of comprehensive preparedness, we need to look beyond military hardware and consider the defence of Europe from a civilian-military and dual-use perspective:

× **The wider set of dual-use infrastructures and capabilities that become vital in a war or crisis require an urgent upgrade**. Here too, Europe needs to make up for lost time since the end of the Cold War. The investment in the trans-European transport network (TEN-T) needed to ensure the swift movement of the military is a case in point. This report has also flagged further dual-use opportunities in relation to space, critical infrastructure, maritime, communications, cyber, etc. within legal and regulatory margins. Moreover, a cultural shift is required within the EU to mainstream civil-military synergies and dual-use potential, rather than keeping defence-related applications and requirements separated from civilian innovation and broader funding options. We simply cannot afford to pay for these artificial limitations any longer.

BOX 12

Military Mobility as a model for an enhanced EU dual-use policy

When an urgent threat emerges at our external borders or beyond, our military needs to be able to react fast and potentially at a large scale. Military forces disembarking at ports in Europe upon arrival from the US, UK or Canada – potentially 100,000 troops with several thousand vehicles – and the units of EU Member States need to able to cross the EU towards external borders as quickly as possible.

Several regulatory processes and infrastructural bottlenecks can slow them down, however:

1. The armed forces cannot move freely within the EU, but need diplomatic permissions to cross Member State borders, which can take several days to obtain in peacetime.
2. Customs procedures and the special permits required to move dangerous goods (like munitions) can equally take time.
3. Very often, roads, railroads, ports, bridges, viaducts, tunnels, airports and other transport infrastructure are not suited for large, heavy military equipment. Taking detours takes additional time and causes potential vulnerabilities.
4. Traffic systems can be hacked or sabotaged by adversaries seeking to impede military movements.
5. Large-scale military forces and their vehicles need to have sufficient fuel supplies, staging areas, rail and road platforms and other logistical facilities throughout their movement.

The EU is addressing all these challenges through its **Military Mobility Action Plans**, in close consultation and coherence with NATO. For example:

× Through the Connecting Europe Facility, the EU supported 95 military mobility transport infrastructure projects across the EU worth EUR 1.74 billion in total. Given the frontloading of the budget in response to Russia's full-scale invasion of Ukraine, the budget foreseen until 2027 has already been exhausted. The high oversubscription rate of the last call for proposals (three to four times) indicates high remaining Member State demand for such transport infrastructure funding.

× Through the European Defence Agency and several PESCO projects, experts work together to harmonise, streamline and speed up procedures for border crossings, customs, etc. The European Defence Fund is supporting the development of a digital secure network for the exchange of military mobility information between national authorities.

Military mobility is an **excellent example of an EU dual-use policy that contributes to our preparedness for major military contingencies and crises, adopting a whole-of-government approach**:

1. A largely civilian sector is identified as a strategic enabler for the military in times of a major crisis, with measures benefiting both civilian and military stakeholders.
2. Military and dual-use requirements identified by Member States are driving the process.
3. Funding is allocated and programmes are implemented by Commission services, with input and contributions from the EEAS (including EU Military Staff), as appropriate.
4. Regulatory improvements, resilience measures, etc., are coordinated across EU-level policies and working groups with Member States.
5. EU-NATO coordination and coherence is ensured through information exchange and structured dialogue.
6. Member States commit to national improvements in a coordinated manner and use the Permanent Structured Cooperation (PESCO) and the European Defence Agency (EDA) to bring experts together.

The revised Trans-European Transport Network (TEN-T) Regulation now includes a provision making it mandatory for Member States to consider military mobility needs when constructing or upgrading infrastructure on the trans-European transport network.

- At the industrial level, dual use is already part of the business model of major companies, for example in the aerospace domain. To maximise industrial capacity and R&D output, the EU needs to **strengthen links between the defence industry and other strategic industrial sectors, not only in aerospace, but also in shipbuilding, for example** (where major external dependencies have emerged, with China dominating the global market). As we further strengthen these industrial ecosystems, ensuring the security of production, supply and information on technology, etc., should be systematically addressed. **The overall requirement of reducing supply chain vulnerabilities and dependencies, enhancing security of supply and diversifying the supplies of raw materials, while building strategic stockpiles, apply a fortiori to the armed forces**. Beyond the primes, the involvement and stimulation of EU's dynamic SMEs is vital in this context too. All this is part of developing an approach that meets the demands of most serious military threats against Europe, while also making sense from the perspective of innovation and strategic autonomy.

- **Moreover, defence organisations need to enhance their resilience and preparedness, including for climate change and the related clean energy transition**. In this regard too, there is an opportunity for enhanced dual-use and civil-military cooperation using the EU framework. The overall trend towards the digitalisation and electrification of our economy will also impact defence capabilities, presenting unique challenges to the armed forces. The low-carbon energy transition can reduce our militaries' dependence on foreign fuel imports and exposure to commodity price shocks, while improving operational effectiveness, ensuring reliable sources of green energy and managing any supply chain dependencies. The US is much further ahead than EU Member States in this regard[23]. **Further EU-level synergies and innovative solutions must be found between Member States, the Commission and the European Defence Agency**[24].

23. For example, the US Army aims to install a micro-grid at every military base by 2035. It has, moreover, formulated an ambition of achieving climate neutrality for its armed forces by 2050, underpinned by a range of strategies and action plans for the different military branches.

24. European Commission and High Representative, Joint Communication on the Climate-Security Nexus, 2023.

Years of underinvestment compounded by regulatory hurdles have negatively affected the innovation capacity of the defence sector, which will have a long-term effect on the EU's comprehensive preparedness.

× **Keeping up with the accelerating pace of defence innovation is vital for Europe to be able to produce the next generation of military capabilities that are already reshaping the battlefield**. This applies especially to the rapid development of automated unmanned vehicles ('drones') that operate in the air, at sea or underwater [see Box 13]. Europe needs to be at the forefront of this development. This means integrating faster paced development and innovation into the capability development processes of the armed forces. It gives another push to the urgent need to better harness overall innovation capacity within the EU, building on the proposals raised by Special Adviser Mario Draghi in his recent report. **This ultimately requires addressing the massive gap in defence innovation investment between the EU and the US, with the latter spending around 11 to 12 times more than both the EU-27 and under relevant EU instruments combined**[25]. In addition, beyond the need to address the defence innovation investment gap, the drone supply chain also provides a useful example of important challenges linked to the security of supply in the defence industrial sector. Figure 12 highlights key players along different stages of the drone supply chain and reveals different security of supply risks, as well as potential bottlenecks along the supply chain.

BOX 13

Unmanned systems – 'drones' – are changing the battlefield

Unmanned systems (or uncrewed systems), often referred to as 'drones' or 'robots', are an increasingly important element on the modern battlefield. They are designed for all military domains, from the air, surface, underwater, and ground, to cyber, and space. They can range from software robots performing automated penetration testing against cyberattacks to uncrewed ground vehicles able to evacuate wounded soldiers from the battlefield and identify the persons in need with the assistance of surveillance and search aerial platforms launched from the ground vehicle.

The Russian war of aggression in Ukraine has brought the potential of drones to the forefront: from the small aerial FPVs (often built from 3D-printed parts) that are used to deliver payloads at a maximum of 50 km away and the medium altitude drones that can fly deep into Russian territory, to the naval systems that have been very successful in attacking the Russian Black Sea fleet[26]. Drones have entered the battlefield en masse, thanks to their availability and low cost. This was witnessed earlier in Myanmar, Libya, Nagorno-Karabakh, Syria, Gaza, Iraq and Afghanistan, to name a few examples. These drones make use of relatively low-level technologies and components, which make them accessible to a growing number of non-State actors. The Houthis in Yemen, with the help of Iran, have conducted 40% of their strikes on shipping in the Red Sea using drones[27].

The phenomena of fast-paced innovation, development and production – sometimes only weeks from lessons identified on the Ukrainian battlefield to new product versions, given the rapid electronic warfare countermeasures against them – present new challenges to armed forces and the wider defence sector. This requires a more agile procurement and development approach than is customarily pursued in the defence sector – a discussion that has also emerged in the US (e.g. in the US defence industrial strategy).

25. See: Draghi, M., The future of European Competitiveness: In-depth analysis and recommendations, 2024, p. 165.

26. Council on Foreign Relations, How the Drone War in Ukraine Is Transforming Conflict, 2024.

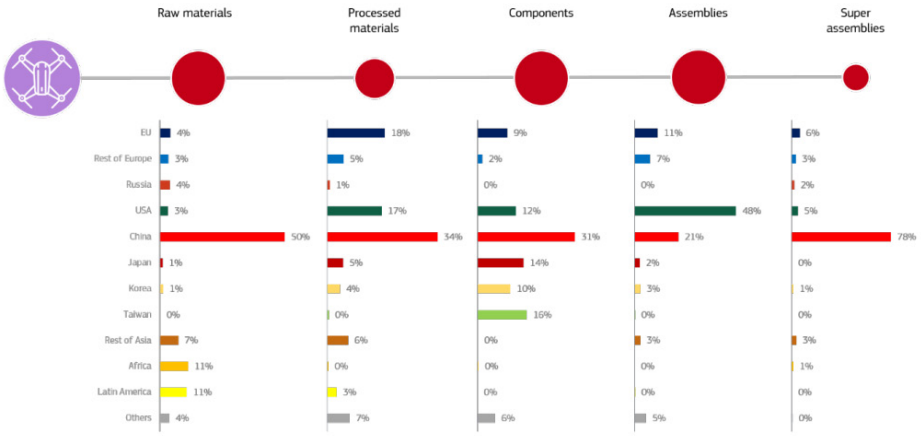
27. ACLED Data, Six Houthi drone warfare strategies: How innovation is shifting the regional balance of power, 2024.

Developments are moving very fast in this domain. Possibly with regional and geostrategic consequences. This applies, as experts have signalled, to the development by the US Air Force of so-called Collaborative Combat Aircraft (CCA): semiautonomous, uncrewed aircraft (UAVs) that could fly alongside fighter jets as a so-called 'loyal wingman'. US officials have stated that the planning assumption is to have 1,000 CCAs by the end of the decade, or two CCAs for each of the 500 advanced fighter jets in the US air force (F-35 and beyond). They are to be powered by jet engines and could potentially be equipped for a variety of missions, including air-to-air combat; air-to-ground combat; electronic warfare; targeting; and intelligence, surveillance, and reconnaissance. They will have an AI-enabled software interface with the crewed jet that will act as its command centre. They are a critical component of the US strategy to preserve air dominance in face of the development of the long-range strike and stealth air combat capabilities by peer-to-peer adversaries. CCAs are roughly one-third the price of fighter jets, have lower maintenance and sustainment costs, and are 'expendable' in war situations[28]. This type of technology, though in a different, lighter variant, is also envisaged as part of the European FCAS programme, although its delivery is foreseen towards the 2040s.

This concept of teaming crewed and uncrewed systems is part of a wider shift towards a 'system of systems', which connects different capabilities in a single digital platform, often enabled by space-based satellites and AI-enabled software. The same applies to the development of naval unmanned vehicles, including for mine countermeasures, but also surveillance tasks where technology is moving towards more and more autonomous features. The counter-drone technology, especially electronic warfare (EW), is equally move forward very quickly, with a range of different challenges from a preparedness and readiness perspective.

FIGURE 11

Overview of the drone supply chains, including shares held by different producing countries/regions



Source: JRC, 2023.

28. Congressional Research Service, U.S. Air Force Collaborative Combat Aircraft (CCA), 2024.

- **Inflexible procurement and budgetary processes, lengthy internal procedures designed for the procurement of complex platforms, and the lack of dual-use research possibilities have created comparatively unfavourable conditions for the EU's defence sector**. The civilian commercial sector is the main driver of high-tech innovation, pioneering the development of key capabilities and applications that are then spun into the defence sector. The latter needs to be able to harness the **much faster civil innovation cycles for technologies with dual-use potential to maintain its competitiveness and ensure the military's edge on the battlefield**. Therefore, to continue filling the innovation pipeline, it is important to invest in cutting-edge civilian technologies that may later develop into defence applications.

- **Not only stronger public-private, but also stronger civil-military cooperation needs to be embedded from a preparedness perspective, wherever possible**. While civil protection, internal security, health security and defence share some overall objectives (the protection of citizens), they each have very different dynamics, different stakeholders and varying mandates and legal frameworks. Yet, greater synergies can and must be found to optimise the use of scarce resources in developing relevant (specialised) capabilities. The prerequisite for promoting synergies between civilian security and defence research and development lies in identifying areas and domains of reciprocal interest for both civil protection, security and defence users (e.g. in the domain of CBRN) and defining technologies and capabilities that are critical for both areas (e.g. from critical communications to sensors and components). Notwithstanding the clear similarities of the three sectors at the technological level, civil security capabilities and requirements are very different than defence/military requirements. In this regard, the EU should further build on its Action Plan on synergies between civilian, defence and space industries[29]

29. European Commission, EU Action Plan on Synergies between civil, defence, and space industries, 2022.

Recommendations

1. **Develop an EU defence capability package for the next decade:**
   - × Use the forthcoming White Paper on the future of European Defence to frame an ambitious long-term ambition and policy, with a view to concrete steps forward.
   - × Fully implement the European Defence Industrial Strategy and the related programme.
   - × Identify and develop, as a matter of urgency, a set of major Defence Projects of Common Interest, underpinned by the necessary ad hoc and long-term budgetary provisions.
   - × Make available the necessary EU-level funding to incentivise and strengthen joint capability investment to prepare Europe for major military contingencies.
2. **Strengthen Europe's capacity to provide mid-to-long-term military assistance to Ukraine.**
3. **Develop the proposed Single Market for Defence with tangible measures to enhance cross-border cooperation and industrial competitiveness.**
4. **Strengthen dual-use and civil-military cooperation at the EU level, based on a whole-of-government approach:**
   - × Conduct a review of the EU's dual-use potential across all relevant domains to identify new synergies, including in space, energy, communication, research, transport, maritime, internal security, etc.
   - × Strengthen dual-use research and defence innovation in the EU framework to stop Europe from lagging further behind the leading powers to the detriment of its long-term strategic position.
   - × Strengthen links between the defence industry and other strategic industrial sectors that form part of the same ecosystem, such as naval/shipbuilding, space, aerospace, etc.
   - × Develop a structured civilian security capability development programme.

1. DEVELOP AN EU DEFENCE CAPABILITY PACKAGE FOR THE NEXT DECADE:

→ Use the forthcoming White Paper on the future of European Defence to frame an ambitious long-term ambition and policy, with a view to concrete steps forward.

- × **Identify and map the urgent defence needs** of Member States and find ways to help address them within the EU framework in complementarity with NATO efforts. This should provide a basis for the development of a long-term goal to drive the EU's capability development and industrial policy, revising the existing EU politico-military Headline Goal to meet the demands of military readiness for a large-scale, multi-domain and protracted external aggression. This should provide a basis to identify possible flagship capability projects, but also address wider whole-of-government including dual-use requirements and opportunities.

- **Strengthen our preparedness and readiness** through a clear and unequivocal commitment from Member States at all levels to plan, invest and operate together as Europeans, as called for in the European Defence Industrial Strategy.

- **Promote mutual reinforcement with NATO activities and standards** in the overall design of major capability domains, ensuring interoperability and enhancing the EU's added value. Concrete and practical steps should be envisaged, building on successful models of EU-NATO cooperation to date, such as the MRTT-project[30] or military mobility.

- **Develop concrete options to enhance EU-level funding** to incentivise and facilitate cooperation, readiness and preparedness in the defence sector, in view of the next MFF and bridging the identified gaps until then. Taking into account the scale and urgency of the task to increase Europe's defence readiness, these solutions should not wait until the beginning of the next MFF in 2028.

- **Provide guidance for the development of the Single Market on Defence**, as set out further below.

- **Strengthen where possible the governance of European defence**, with a view to providing a streamlined toolkit available to Member States and the defence industry. Respecting the institutional balance, the aim should be to put a stronger focus on concrete and timebound deliverables by compelling top-down strategic guidance from the European Council in light of the threat environment. A more integrated suite of mechanisms, tools and instruments, combined with improved coordination and information sharing between the EEAS, the EDA and Commission services, could help to reduce current complexities and partial overlaps. Ultimately, here too a simplification and de-fragmentation effort would be beneficial to ensure a stronger focus on delivery.

→ Fully implement the European Defence Industrial Strategy and the related programme.

The actions set out in this framework and the legislative proposals under the draft European Defence Industrial Programme provide a coherent answer to the long-standing challenges of the defence sector in the EU. It bolsters the aggregation of demand and creates new possibilities to incentivise joint development and procurement, ensuring the security of supply in crisis situations, etc. These proposals provide the best possible answer given the difficult security situation and the fragile state of Europe's undersized and fragmented defence efforts.

→ Identify and develop, as a matter of urgency, a set of major Defence Projects of Common Interest, underpinned by the necessary budgetary provisions.

In conjunction with the White Paper process, and as proposed in the Political Guidelines (2024-2029), work should be conducted with Member States to identify a substantial capability investment package to close the most critical capability gaps. Air defence and cyber defence have already been highlighted in the Political Guidelines as concrete examples.

Within the range of capability priorities agreed by Member States through the CDP and CARD process, which are coherent with NATO's priorities, a selection should be made based on a coherent

30. In December 2013, the European Council identified the Multirole Transport Aircraft (MRTT) as a major flagship initiative to be addressed by the European Defence Agency. MRTT are capable of passenger transport, air-to-air refueling and medical evacuations. Between 2016 and 2018, the first procurement orders by a consortium of Member States were signed at the EDA, working together with the Organisation for Joint Armament Cooperation (OCCAR) and the NATO Support and Procurement Agency (NSPA). In 2023, the fleet of nine (soon to be ten) Airbus A300 MRRT became operational under the ownership of six Member States (Germany, the Netherlands, Belgium, Norway, Luxembourg and the Czech Republic) under a pooling and sharing approach. Participating nations share costs in proportion to their annual flight hours, benefiting from economies of scale. See: European Defence Agency, EDA-initiated multinational fleet of tanker transport now deployable worldwide, 2023.

set of criteria, such as 1) urgency (including in the context of continued support to Ukraine), 2) long-term strategic significance, and 3) industrial and innovative potential within the European Union. These assessments need to be made against a challenging multi-front planning scenario and also address vulnerabilities from a preparedness and readiness perspective, including in terms of the security of supply and the need for ever-warm facilities.

The selected flagships should be future-facing capabilities that can make a strategic difference, both within the EU and NATO and together with Ukraine; offer industrial benefits within Europe based on various ongoing programmes; and help to strengthen our preparedness by meeting the demands for both cutting-edge capabilities, as well as the necessary quantity of weaponry and ammunition that will be needed on a significant scale in a full-scale and protracted conflict. The flagships need to be embedded in a wider NATO and transatlantic planning approach.

BOX 14

Developing a European air defence shield

In today's volatile geopolitical context, **defence against missiles, uncrewed aerial systems (UAS) and other threats in and from the air domain**, is a critical requirement. We see in Ukraine daily how an effective air defence system saves lives and protects critical infrastructure, but also how damaging successful attacks are. Beyond adversarial State actors, non-State actors such as the Houthis in Yemen are developing their capacity to strike with drones at strategic distances, even reaching the southern parts of the EU. And with the lowering threshold other non-State actors, such as terrorist organisations, can potentially use these vehicles as weapons.

It is therefore urgent to step up our efforts to **build and sustain credible 'Anti Access and Area Denial' capability for the Air Domain**, including an integrated air and missile defence system to protect the population, territories and critical infrastructure in Europe. The EU has already identified air and missile defence among key priorities that need to be addressed, with various proposals recently made by European governments alongside different ongoing projects.

Air defence is an area where a **comprehensive system architecture is needed, with different layers and system modules allowing for multi-stakeholder contributions**. The different ongoing and proposed Member State initiatives in this field could mutually complement each other. Collaborative activities are already ongoing in the EU framework are for example within **the EDF and its precursor programmes** (ranging from defence against Hypersonic Missile threats to Low, Small, and Slow threats, i.e. 'mini-drones') and the **PESCO framework** (C-UAS; Timely Warning and Interception with Space-based TheatER; surveillance; Integrated Multi-Layer Air and Missile Defence System). These activities would be in line with and complement NATO initiatives in the area.

Subject to Member States' agreement, a 'European air defence shield' could constitute a European Defence Project of Common Interest, as proposed in EDIS. This flagship could constitute a key contribution to the security and defence of the EU and its Member States, while strengthening the European industrial base and fostering cooperation. Operational command and control systems need to be organised at the national level and within NATO. **The EU can contribute by facilitating the joint development and procurement of material produced in the EU. It can also promote synergies with civil and space surveillance systems, including in the context of border protection**. In the immediate to short term, the procurement of very short-range air defence systems and counter UAS were identified. For the medium-to-long term, the focus could shift to the development of integrated air missile defence systems.

→ Make available the necessary EU-level funding to incentivise and strengthen joint capability investment to prepare Europe for major military contingencies.

The currently available funding from the EU budget for defence-related expenditures is below what is needed in light of the strategic context. The EU's defence related programmes are generally designed to support and facilitate joint and collaborative projects by Member States and/or the defence industry, acting as a 'flywheel' for the rationalisation of Europe's defence sector. However:

- × The overall volume of the available EU budget compared to national budgets is not enough to make a sufficient impact in the market.
- × Compared to the level of underinvestment accumulated over the past decades, Europe still needs to catch up in terms of its defence expenditures[31].
- × Despite the merits of the individual projects, efforts through PESCO, the EDF and other programmes are often too scattered and/or slow-moving.
- × Greater mainstreaming of civil-military and dual-use opportunities would generate a more optimal use of scarce resources.
- × Finally, in some areas such as military mobility, funding has already been completely exhausted.

Overall, the current EU Multiannual Financial Framework (MFF) allocates around 1% of its total of EUR 1.2 trillion to defence (2021-2027). The EUR 1 - 1.5 billion allocated to defence from the EU budget annually is insufficient to impact a defence market of close to EUR 60 billion of Member State spending on research, development and procurement. Current EU budgetary provisions are insufficient to rationalise European defence and to support Member States to work together to strengthen Europe's overall defensive capacity to meet the most extreme military contingencies in the near future, or even offer sufficient to support Ukraine in its defence against the Russian onslaught in the long haul.

The predictable, large-scale and long-term availability of EU funds to support, in line with the Treaties, European defence readiness and capability development is crucial to European defence companies considering new investment to expand their production capacity and private investors who are increasingly examining opportunities in the defence field that has so far remained of marginal interest to them. Companies build additional production lines, commit to new research and development projects and hire more staff (who often need lengthy onsite training) only if they trust that defence will remain a priority in the EU and there is continuing demand for additional supply and a growing market for new innovation in Europe.

2. STRENGTHEN EUROPE'S CAPACITY TO PROVIDE MID-TO-LONG-TERM MILITARY ASSISTANCE TO UKRAINE.

Part and parcel of the EU's defence agenda should be to maintain and further strengthen the capacity to **deliver military support to Ukraine for as long as it takes**. This is critical to keep Ukraine in a position to defend itself against the Russian invasion. The EU and its Member States are already at the top of the donors of military equipment to Ukraine, though there is an ongoing shift from a focus on donations of operational equipment to the procurement of new equipment as stocks and inventories dwindle[32]. This leads to the urgent need to ramp up defence production capacity, as is currently already happing with the production of 155mm artillery shells. The EU

31. The combined EU spending on defence from 1999 to 2021 increased by only 20%, against almost 600% for China and almost 300% for Russia. This is even before Russia massively increased its defence budget over the last two years [see chapter 1].

32. Kiel Institute for the World Economy. Ukraine Support Tracker. 2024.

must also be ready to fill any possible gaps in case of a diminished level of support for Ukraine from the US. It is critical to **ensure the EU can continue to support Ukraine's immediate military needs and continues to function as a platform for military support to Ukraine**, in full complementarity with other international efforts.

To this end, the European Peace Facility, as a flexible, swift off-budget instrument operating under the CFSP should be endowed with sufficient resources. It needs to be accompanied by further measures and incentives to ramp up and speed up defence industrial production in the EU under the relevant instruments. To ensure the reliability of EU military material support to Ukraine in the long term, options should also be envisaged for a support instrument or format that includes only those Member States willing and able to provide this, building on the decisions taken to set up a dedicated Ukraine assistance fund within the EPF. Over the medium-to-long term, the EU should continue to fully support Ukraine's military needs, in a manner coherent with its security commitments agreed with Ukraine. The latter foresee the predictable, efficient, sustainable and long-term provision of military equipment, as well as fostering greater cooperation between respective defence industries.

With Ukraine on its path to EU accession, the EU should better accompany this process and structure its progressive integration into the European defence ecosystem, as envisaged under EDIS and EDIP. Overall, ramping up the production of 155mm ammunition, missile defence systems and logistical support for transferred operational capacities will be critical. Increasingly, this means that **EU defence planning needs to be systematically based on the needs of the EU-27 and Ukraine**.

3. DEVELOP THE PROPOSED SINGLE MARKET FOR DEFENCE WITH TANGIBLE MEASURES TO ENHANCE CROSS-BORDER COOPERATION AND DEFENCE INDUSTRIAL COMPETITIVENESS

Rationalising the defence equipment market in the EU will benefit our competitiveness as well as our security and preparedness. **Currently, there are various ingrained practices, regulatory hurdles and political divergences that stand in the way of a more integrated Single Market for defence**. These are partly inherent to the specificities of the defence sector, in which governments are the only buyers. However, given the limited size of the home market, defence companies are often highly dependent on third market sales. Moreover, Member States often buy outside the EU for various reasons that go beyond the relative performance of EU-produced equipment compared to that of our competitors. **This perpetuates the vicious cycle of Europe's defence fragmentation, its lack of economies of scale, and external dependency**.

Lowering the barriers to cross-border cooperation on both the demand and supply side should help to move EU forward to de-fragment its efforts. This in turn should **reduce the cost inflation of defence products** (which is structurally higher than in commercial sectors), **with a detrimental impact on the purchasing power of national governments**[33].

This requires **disentangling a range of intertwined practices**, which will ultimately help to avoid Member States still feeling compelled to argue for maintaining a high degree of national control over their armament industries. This includes proposals to assure the **security of supply** for defence products (and their maintenance) within the Single Market, the **opening up of cross-border supply chains**, facilitating a harmonisation of **export control policies among Member States including to mitigate their impact within the Single Market** (while noting the impact of the US International Traffic in Arms Regulation (ITAR) regulations for equipment and technologies originating in the US), as well as revisiting the **Public Procurement Directive** [as highlighted in chapter 5] and the **Defence**

33. Defence inflation includes both the overall market inflation rates as they impact the defence sector and the increasing cost of every new generation of defence equipment due to 'gold-plating' (i.e. adding on new capability requirements). For example, real intergenerational cost escalation has been estimated at some 3.5% for naval vessels and 5% to 6% per annum for aircraft and tanks. See: Hartley, K., The Economics of European Defence, 2016.

Procurement Directive, while aiming to further streamline **intra-EU transfers** of defence products where possible (cross-border movements of military equipment within the Single Market still require licensing).

In all these areas, the Single Market for Defence can build on proposals for regulatory improvements and financial incentives made in the context of EDIS and EDIP. It should moreover also find solutions to outstanding constraints related to **access to public and private investment** and finance for military or dual-use goods and technologies. Finally, it should also connect to the wider EU effort to strengthen its innovation potential, including to **pave the way for non-traditional and smaller companies** to take part in the defence sector.

These and other bureaucratic and regulatory hurdles that stand in the way of a faster, ramped-up, more integrated, specialised and innovative EDTIB should be addressed as matter of urgency. Addressing these and other barriers will require thorough dialogue between the EU institutions, Member States, industry and other stakeholders.

4. STRENGTHEN DUAL-USE AND CIVIL-MILITARY COOPERATION AT THE EU LEVEL, BASED ON A WHOLE-OF-GOVERNMENT APPROACH:

→ Conduct a review of the EU's dual-use potential across all relevant domains to identify new synergies, including in space, energy, communication, transport, maritime, internal security, etc.

As identified throughout this report, new opportunities remain to harness civilian-military synergies and dual-use potential, for example through further work on priority (dual-use) transport corridors for military movements; the extension of fuel supply chains for the armed forces along those corridors; stockpiling and strategic reserves of energy, minerals and other critical goods; hospitals and medical services; maritime surveillance and monitoring systems; governmental space-based navigation, communication and observation services; defence energy infrastructure; etc. For instance, time may have come to harvest the benefits of Galileo for defence users. **Galileo Public Regulated Service (PRS) was designed to meet military requirements**: its robustness against radiofrequency interferences ensures its security, accuracy and the continuity of its services. As such, access to Galileo PRS could provide highly resilient positioning, navigation and timing services to armed forces and further facilitate collaborative combat and targeting.

Such an approach could also allow the exploration of new funding possibilities, from within the EU budget and possibly from the EIB. Further examining and harmonising **dual-use definitions in various relevant EU funding instruments and policies** would be conducive to this objective. Within each area, the full extent of legal and regulatory margins should be explored, taking into account the specificities of the sector and defence-related actors respectively. Develop new **civil-military options for pooling capabilities** (e.g. remotely piloted aerial vehicles, border security equipment, specialist emergency response units, heavy lifting transport, etc.), drawing on the rescEU model developed in the Union Civil Protection Mechanism.

→ Strengthen dual-use research and defence innovation in the EU framework to avoid Europe from lagging further behind the leading powers to the detriment of its long-term strategic position.

The recent Commission White Paper on research and development involving technologies with dual-use technologies lays out both the origins of the current separation of civilian and military R&D under EU programmes – and options to remedy the lack of synergies and underused dual-use potential[34]. From a preparedness perspective, it would make sense to consider those options which lead to a) the most optimal use of scarce resources, compared to those available to global compet-

34. European Commission, White paper on options for enhancing support for research and development involving technologies with dual-use potential (COM(2024) 27), 2024.

itors that do not necessarily share our inhibitions, and b) enhanced synergies between defence and civil security applications (such as, in the area of space or autonomous vehicles) in line with the analysis in this report.

Such dual-use R&D needs to be part of a wider ecosystem of disruptive innovators and end users that encourages 'high risk, high return' investment and procurement. Here, we can build further on proposals in the report by Special Adviser Mario Draghi on the Future of European Competitiveness. Moreover, the innovation drive should be applied not only to the capacities to be developed but also the production methods used at the industrial level.

Defence and dual-use-related considerations should be fully embedded in the EU's work on critical (foundational) technologies, such as AI, quantum, etc., especially in terms of promoting the EU's advances in this field to reduce dependencies and protect against technology leakage[35]. Falling behind in the development and application of these technologies means that others will set the standards and gain civil-military and strategic advantages that will be difficult to reverse or overcome. While ensuring the necessary ethical safeguards and international norm-setting, these technologies are key not only from an economic, but also from a wider defence perspective. The use of AI-enabled software is not only powering the drones on the battlefield in Ukraine, but can also support more efficient and effective applications in logistics, targeting, navigation, etc. A study into international benchmarks and best practices from both competitors and partners could be envisaged as a matter of urgency to support a more strategic EU discussion on defence innovation.

There are furthermore important links to efforts towards the Europeanisation of supply chains in the defence sector, through the EDF, with a growing involvement of new players in defence supply chains. The capacity and autonomy to develop innovative defence products must be underpinned by the possibility to offer innovative undertakings — especially start-ups, SMEs, small mid-caps and Research and Technology Organisations (RTOs) — more flexible, faster, and leaner funding cycles, and facilitate better connections with military end users and investors[36]. We can learn lessons from Ukraine in this regard, including through the EU Innovation Office in Kyiv.

In addition, such an ecosystem should foster and facilitate the immediate industrialisation and mass production of validated solutions. This requires bridging the gap between research and innovation on the one hand, and deployable capabilities for the armed forces on the other. Moreover, these efforts have to be underpinned by strong safeguards against foreign interference in EU-funded research (research security safeguards, and some protection of EU-funded research outputs, so they remain beneficial to the EU primarily).

→ Strengthen links between the defence industry and other strategic industrial sectors that form part of the same ecosystem, such as naval/shipbuilding, space, aerospace, etc.

This ultimately allows Europe to retain its high-end industrial capabilities that are vital also from a preparedness, security and defence perspective. It would provide a broader base to ultimately facilitate scaling up defence production and the development of new dual-use products. Here too, civilian-military synergies need to be harnessed, as the defence sector forms part of a broader strategic industrial ecosystem that relies on similar or interchangeable raw materials, technologies, skills, machines, and other industrial infrastructure.

35. The Commission identified ten critical technology areas for the EU's economic security: advanced semi-conductors; artificial intelligence; quantum technologies; biotechnologies; advanced connectivity, navigational and digital technologies; advanced sensing technologies; space and propulsion technologies; energy technologies; robotics and autonomous systems; advanced materials. See: European Commission, Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States (C(2023) 6689 – Annex), 2023.

36. The EU Defence Innovation Scheme (EUDIS), developed under the EDF with a EUR 2 billion budget, provides for innovation support services for single entities, including matchmaking with investors, partners and end-users, and support for product and technology testing and validation. It will work to reduce red tape by exploring the introduction of 'ever-warm' calls for projects and ways to support promising technology transfer from civil to defence, where applicable.

→ Develop a structured civilian security capability development programme.

While the capability/forward-looking approach is well established in defence, it must be set up and promoted at the EU level in the civilian area. Ideally, the coordination of investment in the distinct but parallel areas of the civil security and defence programmes should come from an upfront, structured and institutionalised strategic process. This process would adopt a Capability Driven Approach, starting from an early definition of the key capabilities required, as well as the identification of gaps and needs, up to research, the development and deployment of the required solutions addressing those needs. This process should be supported by consistent EU funding schemes that can accompany this process, as appropriate.

A number of challenges specific to the civil security domain have so far prevented the effective implementation of a capability-driven approach in this area. These are, among others, a highly fragmented ecosystem and a culture focused on short-term needs that hampers addressing uncertainty in a structured, systematic and analytical way. At the EU level, **security and defence users should share their respective operational capability needs and gaps in areas of common interest**. Such a process would however require a structural change in the way the security sector approaches planning, aligning with the best practices of the defence sector, while also learning lessons in terms of agility, standardisation and collaborative effort. A number of enablers that can constitute a solid base for a change of paradigm in strategic programming across EU civil security sectors are already in place, but need to be embedded in civil security planning. Among these are more forward-looking security policies, an institutional push to improve synergies between actors and between funding instruments, a consolidated security research and innovation ecosystem, and growing interaction between buyers and suppliers of EU security technologies.

CHAPTER · CHAPTER · CHAPTER

08

Building mutual resilience with partners through assertive EU diplomacy

‘Mutual resilience’ as the basis for global preparedness partnerships

The EU’s resilience and preparedness at home are intertwined with those of our regional and global partner countries. Many of the threats, risks and challenges set out in this report either originate abroad, have a strong cross-border dimension, or are global and overarching in nature. Preparedness-by-design [see chapter 2] must therefore include proactive and cross-sectoral external action.

In fact, the challenge of strengthening resilience and preparedness in a volatile and increasingly contested world is shared with many if not all our bilateral and multilateral partners. More than that, **many partner countries not only face the same challenges as we do – they are often at the forefront of facing them**. Notably, this refers to Ukraine fighting Russian aggression and defending Europe’s security more broadly, and numerous countries across the Sahel region, the Pacific Ocean and other regions on the front line of the global struggle against climate change. In this sense, Europe can learn a lot from the experiences and best practices of its partners.

The EU should turn its focus on further strengthening mutual resilience with its partners – based on shared interests and in line with our principles and values. The notion of mutual resilience builds further on the ongoing paradigm shift in the way the EU conducts diplomatic outreach and approaches international partnerships. This shift is reflected in the recent Communication on ‘building sustainable international partnerships as a Team Europe’, which takes stock of the progress achieved in revamping the EU’s model of cooperation[01]. It also reinforces the EU’s previous efforts to strengthen a strategic approach to resilience building in EU external action, as it cuts across a

01. European Commission and High Representative, Building sustainable international partnerships as a Team Europe (JOIN (2024) 25 final), 2024.

wide range of sectoral policies, tools and instruments addressing different threats and challenges[02]. Depending on the context and the most pressing requirements of the individual partner, the EU can tailor its contribution to the resilience needs of that partner, ranging from post-conflict reconstruction and economic development to climate adaptation, countering cyber and hybrid threats and enhancing economic security.

Partnerships in an age of strategic competition

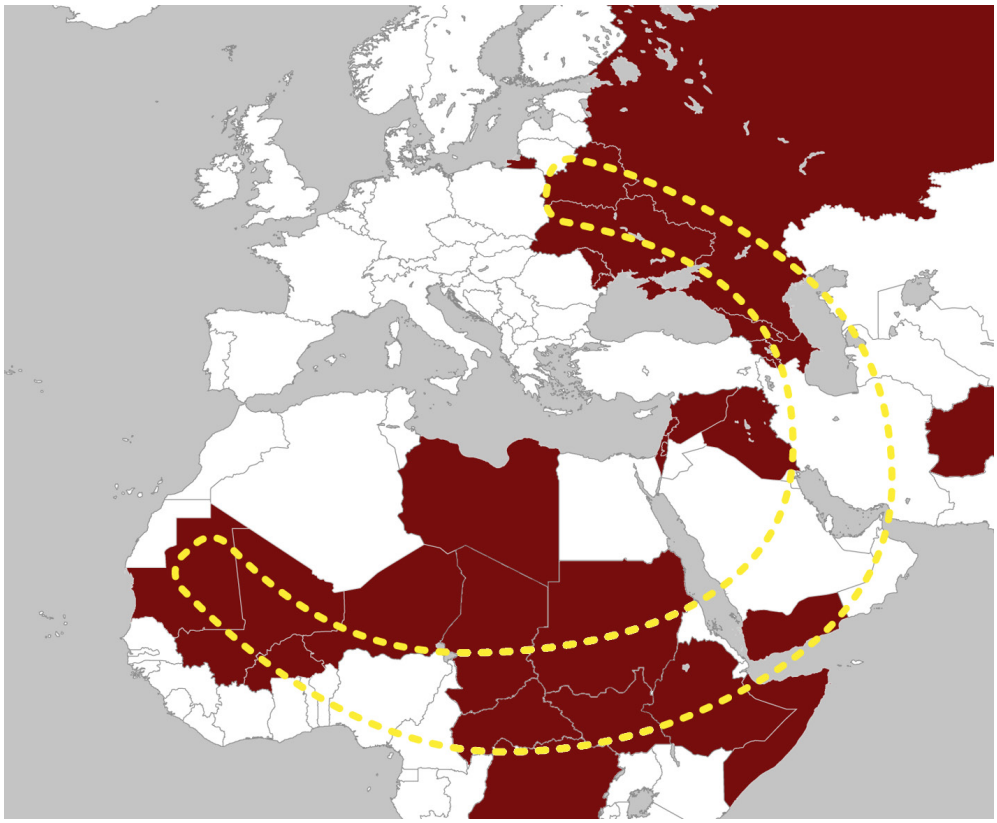
Increasingly, **the EU needs to navigate its international partnerships in the context of all-pervasive strategic competition and contestation that is seeping into every part of the globe and affects many if not all sectors of international partnerships**. From development to conflict resolution, from trade negotiations to connectivity, and from our neighbourhood to partners in the so-called 'Global South', this geopolitical reality is creating complex and often contradictory challenges the EU will need to reconcile as part of its external action:

- **First, the EU has increased its focus on providing a competitive investment offer** to reinforce the resilience of digital, energy, transport, health and education, as well as other infrastructure in partner countries, as marked by the Global Gateway initiative. The EU's offer already brings certain qualitative advantages to the table, as it safeguards social and human rights, promotes sustainable development with a clear local added value and is predicated on transparency and democratic values. Many partners do not always appreciate seeing their partnership projects with the EU framed as part of a global power struggle however – especially when they pursue a non-aligned or multi-partnership foreign policy. Instead, the EU's Global Gateway should rather be framed as enhancing partners' ability to choose the most desirable option available to them. In this sense, the EU's partnership model offers an attractive way to enhance not only the resilience, but also the geopolitical independence of those who prefer not to fully align with any global power.

- **Second, there has been a relative shift away from resilience building in fragile settings**, notably following the range of setbacks in recent years from the Sahel to Afghanistan. Russia and other destabilising actors successfully fed off anti-Western sentiment to create a foothold for themselves, propping up illegitimate regimes in exchange for access to raw materials, while also gaining control over important migratory routes towards Europe. Europe remains a major humanitarian donor, but it has scaled back its security assistance and long-term development cooperation in such countries to avoid legitimising or propping up military juntas or other regimes disregarding fundamental human rights. Nevertheless, the **EU needs to remain present in fragile and politically sensitive settings that challenge our norms and values**, ready to engage in (critical) dialogue and to support vulnerable groups, even if it recalibrates its overall support package. **With war and tensions flaring up in a wide arc to our East and South, the EU faces a particular strategic responsibility to step up its security engagement and conflict resolution efforts**. Although Ukraine and the Middle East are increasingly taking centre stage, the EU also needs to maintain its engagement in Sub-Saharan Africa, despite the growing presence of mercenaries in different countries and the impact of anti-western disinformation campaigns.

02. European Commission and High Representative, A Strategic Approach to Resilience in the EU's external action, 2017.

FIGURE 12
The arc of fragility, conflict, and instability



Source: Based on EEAS, 2024.

× **Third, the EU has always been at the forefront of strengthening effective multilateralism**. However, global cooperation addressing transnational challenges, such as climate change and environmental degradation, the digital transition, the restructuring of developing countries' growing debt load, and even global health, is increasingly affected by strategic competition. Moreover, emerging powers press for a reform of key global institutions, to reflect new economic and demographic realities. Rather than holding on to the status quo, Europe should take the lead in the reform of the international system, taking a positive and proactive role in addressing legitimate concerns, but also to safeguarding core norms and principles on individual rights, democracy and free trade.

Building mutual resilience in a fragmenting global order

Overall, in a fragmenting global order, the EU will need to be more assertive and more active. As a trading power whose legal foundations reflect the principles of international law and diplomacy, the EU remains a crucial defender of the rules-based global order against those who seek to overturn that order through the use or threat of force. The EU depends on its friends and partners around the world to realise this shared vision for a better future in today's more complex world characterised by non-alignment and multi-partnerships approaches. To reinforce and revitalise the international rules-based order – including to shore up the global community's support for Ukraine – the EU should further invest in its global partnerships by diversifying and intensifying its diplomatic engagements.

Yet, the EU should not be complacent about its potential and past accomplishments – the world is changing rapidly. Other players are stepping up their engagement and the EU's relative power is dwindling in light of economic and demographic shifts; hostile disinformation campaigns, for instance in the context of the COVID-19 pandemic or the global food crisis resulting from Russia's invasion of Ukraine. This is further undermining the EU's engagement abroad. The Union should therefore invest in its capacity to serve as a trusted and reliable partner, which provides a long-term perspective, delivers on its commitments in a timely manner, engages in real 'give and take' with its partners and provides a coordinated 'single offer' in the spirit of a true Team Europe approach.

Mutual resilience implies that, while we promote our European interests, we respect those of our partners and are ready to shape our bilateral frameworks by considering their expectations and needs. At the same time, it respects and elevates the EU's partners across the world by acknowledging that their resilience and preparedness is ultimately also in Europe's broader interest. By systematically investing in long-term partnerships, the EU is also shaping external conditions that are conducive to the security, prosperity and resilience of its own citizens, economies and societies. By helping to strengthen our partners' resilience we are also consolidating our own. **Strengthening partners' capacity to prevent, withstand or effectively respond to extreme weather events, health crises, hybrid campaigns, cyberattacks or the flaring up of armed conflict, also lowers the risk of cascading or spill-over effects for Europe**.

From candidate countries to global partners

First and foremost, we should partner on mutual resilience with **EU accession countries and other close regional partners in the EU's immediate neighbourhood. Ukraine's security is our security and therefore Ukraine receives substantive and comprehensive assistance from the European Union**. Beyond Ukraine, reinforcing the resilience and preparedness of other candidates or potential candidates in different areas (e.g. hybrid threats, cybersecurity, climate adaptation and disaster preparedness, economic security, and de-risking) will help the Union to address and patch its own vulnerabilities. Ukraine, Moldova, Türkiye and most of the Western Balkan countries are already full participants in the Union Civil Protection Mechanism, while there are specific well-established regional disaster management partnerships in the neighbourhood that could be built upon. The EU's Security and Defence Partnership with Moldova, and possibly in the future with other countries in our neighbourhood, will contribute to this as well.

The enlargement process allows for structural and in-depth cooperation with candidate countries, including through their gradual integration as they progress towards joining the Union. **Their progressive and merit-based accession to the EU should take into account fundamental questions related to preparedness, including their dependencies and vulnerabilities in relation to external actors**. Similarly, mutual resilience should be a driving principle of our intensifying cooperation with partners in the Southern Neighbourhood. In this vein, different dimensions of preparedness could be addressed through the new Pact for the Mediterranean announced in the President's Political Guidelines (2024-2029).

Mutual resilience and preparedness are also a key building block in our efforts to strengthen the EU's partnerships, starting with **longstanding allies and partners**, such as the US, Canada, Norway, the UK, Japan, South Korea, and Australia. The EU's new Security and Defence Partnership with Norway further showcases this. Working together with like-minded partners helps to draw up coordinated responses, to share lessons and seek opportunities to collaborate.

However, given the global nature of the threats and challenges we face, the Union must also further **strengthen its ties and build mutual resilience with new and emerging partners across the globe**. The advantages here are very similar for both sides. There is an extensive list of potential partners with whom to engage further on mutual resilience, should there be an interest on both sides, often

building on foundations and strategic partnerships put in place in the past years. A prominent example is the EU's enhanced partnership with India, including through various dialogues and the Trade and Technology Council established in recent years.

In this vein, we also need to continue **enhancing dialogues and cooperation on resilience and preparedness with partners at the multilateral level**, including through key multilateral and regional organisations, such as the United Nations (UN), the African Union (AU), ASEAN, the Gulf Cooperation Council (GCC), the Community of Latin American and Caribbean States (CELAC), as well as the G7 and G20. For instance, especially since the pandemic, health security and pandemic preparedness, including through healthcare service capacity building and the scaling-up of local manufacturing of health products, has been a priority for EU-AU cooperation. In addition, while the EU-NATO strategic dialogue on resilience focuses mainly on the internal dimension, the inclusion of external aspects could also be explored.

Working together on common challenges

The EU and its partners share a need for stronger resilience to face, for example, the following challenges:

→ The widening arc of instability, fragility, and insecurity in Europe's vicinity and beyond:

Several areas in the EU's vicinity and beyond are marked by political instability, socio-economic fragility, and ongoing or frozen conflicts, amplifying the spill-over effects that highlight the growing interconnections between the EU's security and the resilience of its neighbours and partners. The persistence of long-running, unresolved conflicts and foreign interference by Russia and other authoritarian actors not only takes a terrible toll on people's lives, but also offers fertile ground to armed groups, terrorist organisations and organised crime. Climate change is exacerbating the potential for instability, security risks and even conflict as competition for scarce natural resources mounts, including in EU's neighbourhood.

→ The broad societal and security impact of climate change:

The most vulnerable countries and people, for example in regions such as the Sahel, are those most severely impacted by cycles of extreme weather events, notably heatwaves, droughts and floods. This has a broad societal impact in terms of water and food security, public health, critical infrastructure resilience, and financial and economic stability. Since 2008, annually a staggering 21.5 million people have faced forced displacement due to extreme weather-related events. It is predicted that over the longer term, without decisive global climate mitigation action, climate change will exacerbate migration pressures as vast areas become unliveable. This will create additional challenges for countries of origin, transit, and destination. In the context of a fragmenting global order, international cooperation to address major transnational challenges, such as climate change, is steadily eroding.

→ The growing threat posed by organised cross-border crime and drug trafficking:

Cross-border organised crime, for instance in relation to drug trafficking, poses a growing transnational security threat shared by the EU and other countries. Over the past decade, there has been a marked increase in global drug seizures. In the EU, between 2012 and 2022, drug seizures spiked for cocaine (+376%), methamphetamine (+293%), cannabis (+184%), and other substances[03]. Euro-

03. European Drugs Agency, European Drug Report, 2024.

pean drug producers and traffickers are closely linked with international criminal networks. Overall, drug-related criminality has become more and more violent in recent years, exacerbating human insecurity and destabilising communities both in the EU and across countries in South America, West and South Asia and North Africa. Beyond drugs, the issues of firearms smuggling and the trafficking of human beings pose growing transnational challenges.

→ **External economic over-dependencies and exposure to supply chain shocks:**

Both the COVID-19 pandemic and Russia's war of aggression against Ukraine have exposed – not only for the EU but also for others – the significant risks and painful consequences of overly depending on individual third countries for critical goods and raw materials. In the wake of COVID-19, critical shortages of personal protective equipment (PPE) and semiconductors undermined the public health response, and paralysed manufacturing in key sectors. Russia's full-scale invasion of Ukraine sparked an energy crisis in the EU, while also precipitating global food insecurity through deliberate distortions of Ukrainian grain exports and other supply chains (for example, for fertilisers). As the EU moves forward with de-risking and supply chain diversification, among other things by forging new partnerships on the energy, defence and raw materials value chains (including the upcoming Clean Trade and Investment Partnerships - CTIP), there is scope to cooperate further and at the same time to strengthen our economic security and that of our partners.

→ **Collectively maintaining secure and open access to key global commons and strategic domains, such as the high seas, outer space, global communication infrastructure, and cyberspace:**

Open and secure access to global commons and strategic domains is vital for the EU and for our partners' security and prosperity. Growing geopolitical contestation and widening instability are increasingly putting this at risk. For instance, the impact of the war in Ukraine on the Black Sea and the recent attacks on commercial ships in the Red Sea highlight the EU and partners' shared strategic interest in safeguarding shipping routes that connect Europe with other parts of the world and in particular the Indo-Pacific. Maritime supply routes and undersea cables are not just commercial lifelines, they are pivotal in times of crisis[04]. Ensuring their uninterrupted functioning is a common objective that underscores the shared importance of effective multilateralism to address these challenges, while strengthening the resilience of global communication infrastructure and better coordinating the international response to emerging threats.

Reinforcing the EU's existing toolbox

As a comprehensive global actor, the EU can build on a rich and broad range of tools and instruments to work with partners to build mutual resilience, for example:

× In the field of **hybrid threats, cyber, and Foreign Information Manipulation and Interference (FIMI)**, regional and bilateral EU programmes, such as the Technical Assistance and Information Exchange instrument (TAIEX), provide policy implementation support and capacity building, especially in the neighbourhood, but also globally. The EU has also launched a comprehensive critical infrastructure protection programme in the Western Balkans. The EU also supports partners through a wide portfolio of cyber capacity building programmes, amounting to over EUR 65 million. Thematic dialogues, for instance on cyber, provide a key platform to identify further avenues for cooperation.

04. More than 80% of global trade by volume depends on maritime shipping and up to 99% of the world's global data flow is transmitted via undersea cables. See: European Commission and High Representative: An enhanced EU Maritime Security Strategy for evolving maritime threats(JOIN(2023) 8 final), 2023.

- In the **field of maritime security**, the EU has long partnered with countries and regional organisations in West Africa, the Red Sea/Horn of Africa and in the Indo-Pacific to counter illicit maritime activity, to support maritime domain awareness and capacity building, and improve maritime security. CSDP naval operations and Coordinated Maritime Presences meanwhile contribute to maritime security in the South-Central Mediterranean, the Red Sea, off the coast of Somalia, and in the Northwestern Indian Ocean. The latter two help to protect commercial shipping lanes that connect Europe with Asia, while the former is essential to disrupt the business model of migrant smugglers to Europe.

FIGURE 13

EU CSDP missions and operations around the world (2024)

Source: EEAS, 2024.

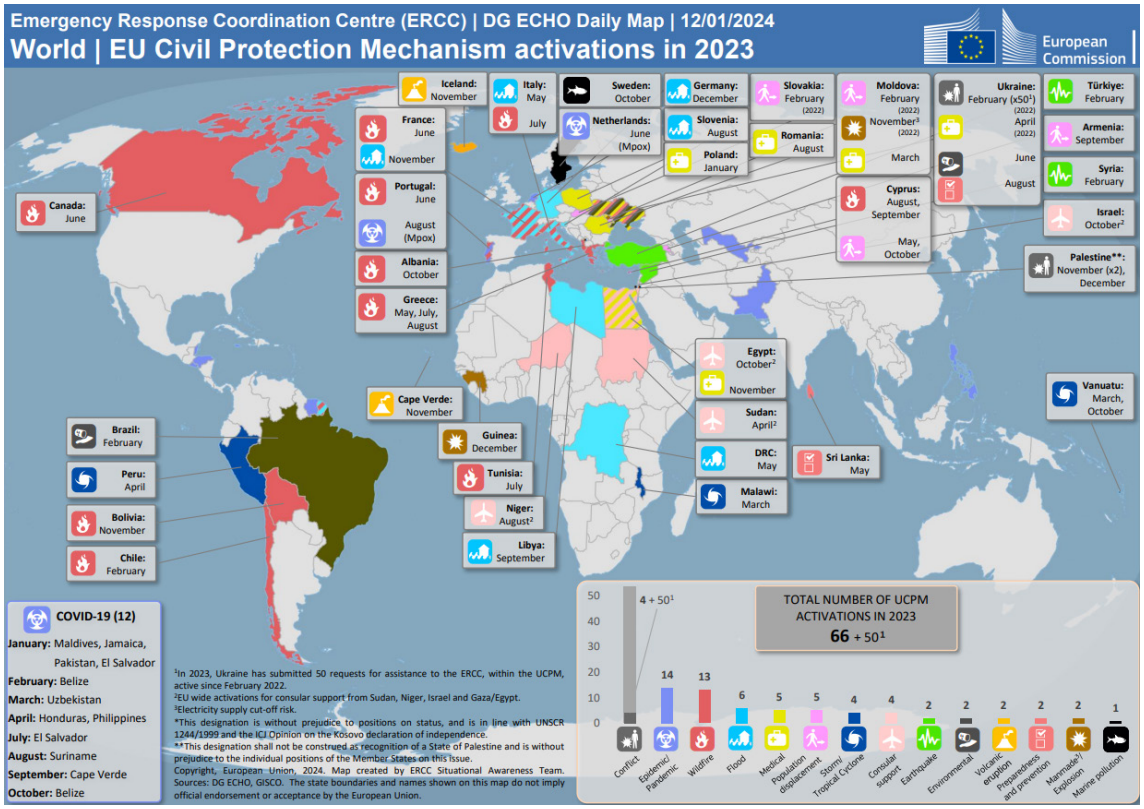
- In the **field of disaster risk management, response and civil protection**, the EU is engaged with partners on both preparedness (e.g. through its initiatives Prevention Preparedness Response to natural and man-made Disasters (PPRD) for the Mediterranean and PPRD East) and emergency response, as well as in multilateral efforts on Disaster Risk Reduction and Early Warning. For instance, 76 out of 106 Union Civil Protection Mechanism (UCPM) activations in 2022 came from outside the EU. In addition, between 2022 and 2024, the UCPM experienced a significant expansion with Albania, Bosnia and Herzegovina, Moldova, and Ukraine becoming Participating States. Beyond the neighbourhood, the EU also invests in disaster risk reduction globally and cooperates with regional disaster management organisations, for instance in the context of the EU-LAC MoU on disaster preparedness and disaster risk reduction.

- In the field of global climate action, **the EU continues to lead in promoting ambitious multilateral efforts to cut global greenhouse gas emissions**, for instance in the context of the annual Conference of the Parties (COP). In addition, the EU works with numerous non-EU countries bilaterally, including on climate adaptation. Together with Member States, the EIB and the UK, EU is the largest contributor of public climate finance to developing economies, providing EUR 28.5 billion in 2022.

× **The EU is one of the largest providers of humanitarian assistance** to the world's most vulnerable people facing conflict or disaster, upholding humanitarian values and principles. In 2023, the EU provided more than EUR 2.4 billion in needs-based humanitarian assistance, working with UN agencies, international NGOs and local partners to support people in crisis situations in 114 countries. With increased fragility and the intensifying impact of climate change, basic humanitarian needs are growing exponentially. To this end, the EU is also engaging in multilateral humanitarian diplomacy to encourage more partner countries to step up to provide principled life-saving aid and to invest in resilience.

FIGURE 14

Union Civil Protection Mechanism activations worldwide in 2023



Source: DG ECHO, 2024.

× In the **field of health security**, the EU led the multilateral response to the COVID-19 pandemic. For instance, it mobilised EUR 46 billion in a Team Europe approach to support partner countries globally both with the immediate response to the health emergency and with strengthening health preparedness and response systems. Similarly, under the Global Gateway strategy, the EU and Member States are continuing to strengthen healthcare capacities around the world, and to invest in the security of pharmaceutical supply chains. For instance, as part of a Team Europe initiative, over EUR 2 billion was mobilised to support the AU's 2040 goal to promote local vaccine manufacturing.

× In relation to sustainable **connectivity and supply chain resilience**, the EU works with partners worldwide to build effective, sustainable and shock-resilient transport corridors and hubs. Notably, the development of the Trans-Caspian Transport Corridor aims to establish a modern, competitive, sustainable and efficient route connecting Europe and Asia in no more than 15 days. To this end, the EU committed to invest EUR 10 billion in sustainable transport connectivity in Central Asia. Similarly, the EU and Member States are investing in the modernisation of critical maritime hubs, such as the port of Cotonou. The Lobito corridor, another flagship under the Global Gateway, will enhance the export possibilities for the Democratic Republic of Congo, Zambia and Angola.

FIGURE 15

The projected Lobito Corridor between Zambia, the DRC, and Angola

Source: DG INTPA, JRC, 2024.

× Moreover, the EU cooperates with partners on **space policy and leverages space-based services to support them on climate change adaptation, disaster risk management, environmental action, and food security**. In 2023, the EU launched the EU-Africa Space Programme to support the African Union's newly created Africa Space Agency, to reinforce the African space private sector ecosystem and EU-Africa industrial cooperation, and to enhance regional early warning capacities. As another example, the EU has set up national and regional Copernicus centres in the Philippines and Panama, providing services for disaster risk reduction, disaster recovery and climate adaptation based on open earth observation data and geospatial technology.

BOX 15

Cyber resilience initiatives with partner countries

The EU and partner countries share challenges linked to malicious cyber activities. Cyber capacity building is a key component of the EU's partnership offer. In particular, this covers four pillars:

1. The development and implementation of policy, regulatory and normative frameworks to protect critical infrastructure, to advance incident-response mechanisms, and enhance cyber literacy and cyber hygiene.
2. Cooperation with law enforcement and judicial authorities to tackle cybercrime.
3. Support to armed forces to enhance cyber defence capabilities.
4. Engagement with diplomatic communities to ensure meaningful participation in inclusive multilateral processes.

Under the Global Gateway, the EU is conducting relevant activities through programmes, such as Safe Digital Boost Africa (EUR 30 million cybersecurity component), the LAC Digital Alliance (working hand-in-hand with the Latin America and Caribbean Cyber Competence Centre), the Team Europe initiative on Secure Connectivity for Central Asia. Through the Multilateralism & Digitalisation programme, the EU co-finances with Estonia the Tallinn Summer School of Cyber Diplomacy.

In addition, the EU has so far signed comprehensive Digital Economy Packages mainstreaming cybersecurity in projects with Nigeria, Colombia, the Democratic Republic of the Congo, the Philippines, and Kenya. Other packages are under preparation with Tanzania, Senegal, Mozambique, Chile, and Jamaica.

Addressing gaps in our approach

The EU needs to further build on broad ongoing cooperation to draw up a positive regional and global agenda which highlights mutual resilience and preparedness, and strategically leverages all of the EU's external action and partnership tools in an **integrated 'whole of the EU' approach**. Taking our approach to partnerships to the next level also means **acknowledging untapped potential and addressing relevant gaps in our approach**.

An EU that effectively engages with partners in building mutual resilience needs to become more:

→ Diplomatic:

To engage new and emerging partners in a long-term effort to build mutual resilience, **the EU should further invest in its convening power and diplomatic outreach at all levels**. The aim is not just to 'listen', but to better integrate partners' needs, expectations and sensitivities in the design of the partnership package. Multi-alignment should not be considered problematic as such, unless enhanced security ties with certain foreign actors in a given country would compromise the EU's possible overall cooperation with the authorities – in this case building mutual resilience would be difficult. While commitment to our values and principles is key for the EU, we should be more flexible in accepting that partners will not be aligned with us on all international issues. Moreover, when facing problematic political settings in a given country, the EU will need to recalibrate its engagement to remain in dialogue with the authorities, without legitimising the military junta or unrecognised government, to promote and defend EU values and interests and maintain projects that benefit the population, especially the most vulnerable groups. Proactive outreach, communication and public diplomacy are essential to identify needs, explain one's intentions and interests, and build credibility. Reducing others' dependencies and vulnerabilities in key sectors can help us to reduce our own.

→ Strategic:

While the EU faces multiple interlocking challenges for its preparedness across different sectors and geographies, we need to become more strategic in our engagement with partners and to avoid the risk of being stretched too thinly. Being strategic means not only adopting a forward-looking and anticipatory approach to building mutual resilience, but also carefully considering most pressing interests, and setting clear priorities for our actions, funding and resources. Our actions across different sectors should be better coordinated to ensure they are mutually reinforcing in promoting our strategic interests. Being strategic also means identifying the most capable and credible partners to work with, depending on their criticality concerning various issues.

→ Smart:

The EU should focus its offer on where it can bring the greatest added value, rather than competing where we cannot effectively do so. Depending on what the partners' main priorities are in view of augmenting their resilience and preparedness, this means drawing on and communicating more actively our specific strengths and experiences, for instance regarding regulation and standard setting, market integration, capacity building, social protection, and principled international humanitarian assistance.

→ Fast:

To be a credible partner and encourage partners to work with us on building resilience, the EU needs to become more agile and to start delivering faster. In a fast-moving and contested geopolitical environment, EU instruments need to remain fit for purpose and geared to address key challenges in a timely manner. This includes ensuring the necessary flexibility of the governance and financial architecture of flagship initiatives, such as the Global Gateway. Similarly, we should consider how we can use our leverage in international financial institutions to accelerate lending and grant allocation processes in the interest of overall effectiveness[05].

05. For instance, over the past five years, World Bank projects have taken an average of 456 days to move from proposal to disbursement. See: European Council on Foreign Relations, Multilateral development: How Europeans can get real with the global south, 2023.

Recommendations

1. **Embed the mutual resilience principle in upcoming EU policy initiatives – taking into account sectoral or regional specificities.**

2. **Use scenario-based risk assessments to prepare EU crisis response options and guide wider policy development on possible external shocks and crises.**

3. **Strengthen outreach and diplomacy to involve and engage with partners at all levels:**
   - × Invest in the EU's convening power and intensify diplomatic engagement at all levels.
   - × Promote mutual resilience by working through multilateral fora and supporting the UN's agenda for the future.
   - × Expand the availability of EU-level early warning tools and instruments to partners.
   - × Strengthen a structural exchange of expertise, best practices and training on mutual resilience through sectoral dialogues and the set-up of regional 'Mutual Resilience Centres'.

4. **Conduct a horizontal stock-taking and mapping of overlapping mutual resilience interests and collaborative opportunities with partner countries as part of the planning for the next MFF.**

5. **Plan better, deliver faster:**
   - × Review and reform processes, tools and instruments to ensure faster delivery.
   - × As part of an upgraded Team Europe approach, promote joint strategic planning between the EU and Member States in relation to mutual resilience and the external dimension of preparedness.
   - × Embed resilience-building and preparedness into the strategic planning for the EU's flagship Global Gateway Strategy.

6. **Strengthen the EU's responsiveness to rapidly evolving crisis situations, including in fragile settings:**
   - × Further reinforce the role of EU CSDP missions and operations and coordinated maritime presences to enhance mutual resilience, including to safeguard international shipping routes and critical infrastructure.
   - × Develop an integrated EU approach to address the arc of instability and fragility in the EU's wider neighbourhood and tackle knock-on effects on European security and stability.
   - × Ensure that international climate finance mechanisms are designed to reach the most climate-vulnerable countries and communities; and reinforce EU assistance to help address the growing consequences of conflict and disasters.

To operationalise the broad concept of mutual resilience – in view of the imminent start of the new policy cycle and the upcoming negotiations for the next Multi-Annual Financial Framework – a number of consecutive and parallel steps should be considered:

1. EMBED THE MUTUAL RESILIENCE PRINCIPLE IN UPCOMING EU POLICY INITIATIVES – TAKING INTO ACCOUNT SECTORAL OR REGIONAL SPECIFICITIES.

This could be based on horizontal parameters, such as:

- An extrapolation of the EU's interests and priorities in external resilience building, drawing on internal work to identify vulnerabilities, risks and opportunities as part of enhancing the EU's preparedness and readiness within and across all relevant sectors.
- An iterative diplomatic process to survey the relevant risks and vulnerabilities faced by the partner country, in cooperation with the authorities of the partner country and relevant EU actors where possible, to identify the partner's resilience needs, including in the context of global and regional developments.
- A whole-of-government and whole-of-society approach that looks at interdependencies across sectors, as well as between the EU and the partner country in question, and potential impacts for the partner country's economy, society and citizens, identifying critical nodes, bottlenecks and tipping points.

While acknowledging the very different settings of individual sectoral policies, applying these key parameters would allow mutual resilience to be integrated by design into the Preparedness Union Strategy, the White Paper on Defence, the new Internal Security Strategy, the upcoming European Climate Adaptation Plan, the New Economic Foreign Policy, the Clean Industrial Deal, and an upgraded Global Gateway Strategy, as well as other future work strands and initiatives sketched out in the new Political Guidelines.

Moreover, mutual resilience should be applied to the EU's further work on cybersecurity, health security, countering hybrid threats, water resilience, research and innovation, the gradual integration of accession partners as part of the enlargement process, and new external strategies towards the Mediterranean, Black Sea, Africa, India, Middle East and East Asian partners. The aim would be to establish mutual resilience as an organising principle for EU diplomacy, external action, and programming across policy domains.

2. USE SCENARIO-BASED RISK ASSESSMENTS TO PREPARE EU CRISIS RESPONSE OPTIONS AND TO GUIDE WIDER POLICY DEVELOPMENT ON POSSIBLE EXTERNAL SHOCKS AND CRISES.

In a volatile world, our preparedness is served by more proactively anticipating possible external crisis scenarios and how they would play out for Europe's security, economy and society. Such scenarios can be politically sensitive and must be handled with the necessary discretion. Moreover, scenario-based risk assessments can be resource-intensive, so they should be targeted to carefully chosen priority issues. For instance, this could include focussing on more immediate issues, in the light of a build up of the potential for conflict in certain geopolitical hotspots with direct implications for the EU. A wide range of different stakeholders within Commission services, the EEAS and other relevant bodies should be involved in the process. The resulting risk assessments should then feed into prudent reflections – involving Member States where appropriate – on concrete crisis response options, to be activated through the appropriate mechanisms if the crisis manifests itself, as well as into wider EU policy development, for example in the context of civil protection, CFSP, security and defence, and economic security.

3. STRENGTHEN OUTREACH AND DIPLOMACY TO INVOLVE AND ENGAGE WITH PARTNERS AT ALL LEVELS:

→ Invest in the EU's convening power and intensify diplomatic engagement at all levels.

Drawing on the EU's extensive global network of delegations alongside high level visits and exchanges, the EU should reach out more proactively and systematically at all levels to communicate a clear commitment to developing mutual resilience partnerships and to rebuild long-term trust. Strengthening coordination of high-level engagements between the EU institutions and Member States and other joint outreach efforts would be vital to ensure a stronger and more coherent European message. This could include organising with partner countries a series of regional mutual resilience conferences, co-hosted by the HR/VP and Member States in a Team Europe approach together with a partner of choice in the region. Such conferences could help to set the tone for future cooperation on mutual resilience, for instance by identifying shared interests and a joint strategic agenda.

→ Promote mutual resilience by working through multilateral fora and supporting the UN's Pact for the Future.

While the focus in this chapter lies on the EU's bilateral work with partner countries, there is a clear opportunity to address mutual resilience through relevant multilateral fora and regional formats, as well as relevant global (financial) institutions and actors. Addressing broader risks, challenges and resilience questions from a multilateral and regional perspective can help to harmonise policy approaches, exchange best practices, set requirements, define standards, generate or coordinate funding streams, and have an important multiplier effect for bilateral partnerships.

The EU's – but also partner countries' – ability to prepare for and withstand external shocks and crisis depends to a large extent on our capacity to leverage international cooperation and multilateral fora to address their root causes and build resilience. EU diplomacy should therefore remain geared towards strengthening the capacity of relevant international institutions, including in particular the UN system, to support and coordinate global efforts on mutual resilience. In this regard, the EU should further contribute to the implementation of relevant actions envisaged as part of the UN Pact for the Future, adopted in September 2024. It identifies a range of actions that are relevant from a mutual resilience perspective, including foreseeing a 'more coherent, cooperative coordinated and multidimensional international response to complex global shocks and the central role of the United Nations in this regard'[06]. The EU and partner countries' worldwide have a shared interest in ensuring that the UN's organs that are responsible for and contribute to the maintenance of international peace and security are effective and well-functioning, despite the well-known diplomatic blockages. This links into the wider set of issues related to the proposed reform of the UN system, for which the EU should be in the forefront.

→ Expand the availability of EU-level early warning tools and instruments to partners.

The EU and Member States have developed a range of tools and instruments to support threat detection and early warning. Many of these are already being employed as part of partnership engagements. In addition, the EU supports the UN's 'Early Warnings 4 All' initiative and has committed itself to promoting universal coverage of multi-hazard early warning systems by 2027 as part of the UN's Pact for the Future. Expanding on this, the EU could further cooperate with partners

06. Of note, the Pact for the Future warns that: 'Complex global shocks are events that have severely disruptive and adverse consequences for a significant proportion of countries and the global population, and that lead to impacts across multiple sectors, requiring a multidimensional and whole-of-government, whole-of-society response. Complex global shocks have a disproportionate impact on the poorest and most vulnerable people in the world and usually have disastrous consequences for sustainable development and prosperity. An armed conflict does not by itself constitute a complex global shock, but conflict could, in some cases, lead to impacts across multiple sectors.' See: United Nations General Assembly. The Pact for the Future. 2024.

on early warning and anticipatory analysis, making further tools available where it is in the mutual interest – not only concerning conflict prevention, disaster response and climate adaptation, but also hybrid threats and economic security.

→ **Strengthen a structural exchange of expertise, best practices and training on mutual resilience through sectoral dialogues and the set-up of regional 'Mutual Resilience Centres'.**

Resilience building with partners requires a continuous exchange of ideas, concepts, best practices, experiences and assessments. This can build on sectoral dialogues, platforms and networks, which should be further incentivised and equipped to deliver concrete projects linked to EU-level funding opportunities. For example, the EU should further roll out the new Security and Defence Partnerships, possibly including elements linked to preparedness more broadly, and offering links to wider sectoral cooperation. To facilitate cross-sectoral and comprehensive exchanges that enhance bilateral and regional cooperation with regard to different dimensions of resilience and preparedness, the EU should consider working with partners to set up a network of regional Mutual Resilience Centres. These Centres would not stand in the way of other cooperation channels and could start as virtual hubs and knowledge sharing platforms, connecting the dots and facilitating knowledge sharing across relevant domains. Using a modular or network approach, they could link to sectoral cooperation centres and hubs, such as the Copernicus Centres in Panama and Chile and the Copernicus mirror site in the Philippines, or other relevant services and expertise from across the EU and its Member States. They could, for example, support dialogues on issues of mutual interest, such as the protection of critical transnational infrastructure or countering hybrid threats (e.g. with Indo-Pacific partners).

4. CONDUCT A HORIZONTAL STOCK-TAKING AND MAPPING OF THE OVERLAPPING MUTUAL RESILIENCE INTERESTS AND COLLABORATIVE OPPORTUNITIES WITH PARTNER COUNTRIES AS PART OF THE PLANNING FOR THE NEXT MFF:

In the course of 2025, ahead of the next MFF, the EEAS and Commission services, together with Member States, should take stock of ongoing actions and envisioned needs in the context of mutual resilience, in different policy and geographical clusters. This gap analysis should pave the way for a greater strategic focus and enable a number of practical, regulatory and funding improvements:

- Enhancing the flexibility of the EU's instruments and further tailoring its partnership offer to partners' expectations and needs.
- Preparing comprehensive partnership packages for the individual partner countries, tailored to their resilience needs and reflecting shared interests.
- Providing a basis for better coordination and possible synergies between different EU sectoral policies. On the basis of an up-to-date overall risk assessment [see chapter 2], anticipatory analysis and strategic foresight, the EU needs to connect the dots within and between economic resilience, climate change, migration, protracted conflicts, hybrid threats, health security and critical raw materials, components and infrastructures.
- Identifying where to prioritise action through existing instruments or to strengthen the EU toolbox to address partners' evolving needs, focusing on areas where the EU has a comparative advantage or a compelling interest.
- As part of the next Multiannual Financial Framework, explore designing external financing instrument(s) that integrate(s) the principles of mutual resilience and preparedness-by-design from the outset.

- Further enabling sectoral engagements under the Global Gateway strategy by developing, as appropriate, dedicated financing options to strengthen the external dimension of core policy domains, such as energy, climate, cyber, health, digital, and involving all relevant sectoral services more closely as part of a whole-of-Commission approach to our partnerships. While using Official Development Assistance (ODA) funds wherever possible, the need for dedicated tools to flexibly promote strategic investments in key partner countries, including in particular middle-income countries, and at scale should be further explored.

5. PLAN BETTER, DELIVER FASTER:

→ Review and reform processes, tools and instruments to ensure faster delivery.

Delivering faster on our commitments and agreed-upon partnership projects helps not only to reinforce mutual resilience at a higher pace, but also adds to the credibility and effectiveness of the EU's global engagement. The EU needs to be able to move faster from the identification of a common interest to providing the funding and launching concrete work. Speed is increasingly a determining factor for the EU's impact and leverage in a fast-paced and crisis-prone geopolitical world. Geopolitical competitors can outpace us with their direct control over their economic and security actors. This requires an effort across the EU (including between institutions, for instance to accelerate the ratification of international agreements) and Member States to enhance analysis and anticipation, procedural and budgetary flexibility, and institutional preparedness, as well as to design responsive tools, instruments and coordination frameworks.

→ As part of an upgraded Team Europe approach, promote joint strategic planning between the EU and Member States in relation to mutual resilience and the external dimension of preparedness.

In response to the COVID-19 pandemic, the EU launched the Team Europe approach in 2020 to foster coordination and coherence, to pool resources and expertise between the EU, Member States, the EIB and the EBRD, and ensure effectiveness and greater impact across all facets of the EU's external action, in particular in the context of the roll-out of the Global Gateway[07]. So far, the new approach has already resulted in 160 Team Europe initiatives (TEI)[08]. Building on these, the EU should now:

- Leverage the Team Europe approach to promote Member States' active involvement in the external dimension of EU preparedness;
- Draw on the principles of mutual resilience and preparedness-by-design to reinforce the strategic orientation of the Team Europe approach, long-term planning, and prioritisation.

This would not only enhance the efficient use of EU and Member State resources and help to maximise the impact of TEIs, but also **strengthen our messaging coherence, overall partnership offer, and leverage vis-à-vis partners**. Enhanced coordination would enable the EU and Member States to better pool, prioritise, and deploy their resources in line with the EU's strategic interests and respond with greater agility to partners' needs and expectations. In this context, the EU and Member States could also explore the need for common governance structures to better align as well as coordinate TEIs and other external programmes aiming to build mutual resilience in the long term.

→ Embed resilience-building and preparedness into the strategic planning for the EU's flagship Global Gateway strategy.

Across all five key thematic areas of the Global Gateway (digital, climate and energy, education and research, health, and transport), the EU should make sure that relevant projects and initia-

07. European Commission and High Representative, Building sustainable international partnerships as a Team Europe (JOIN (2024) 25 final), 2024.

08. European Union, Team Europe Initiatives and Joint Programming Tracker, 2024.

tives contribute to building resilience and crisis preparedness – in line with the objectives of EU external action and partners' interests. For instance, this could include further mainstreaming cybersecurity capacity building measures across the Global Gateway's digital pillar, as well as other areas of cooperation, such as health, education, and transport. Similarly, Global Gateway could further strengthen the provision of space-based monitoring and information processing services to enhance partners' all-hazards preparedness. This would feed into an overall support package that combines EU, Member State and private investment with technical assistance, joint training and policy dialogues on digital commons and standards, trusted connectivity, cybersecurity, data governance, human-centred e-government, education and skills' development.

6. STRENGTHEN EU RESPONSIVENESS TO RAPIDLY EVOLVING CRISIS SITUATIONS, INCLUDING IN FRAGILE SETTINGS.

As part of its own preparedness and ability to support partners, the EU needs to be ready to respond to unfolding external crises, using its full-spectrum toolbox, including the Common Security and Defence Policy. This is very often our 'first line of defence' to avoid that external situations deteriorate, escalate or spiral further, with potentially even worse impacts on the local population and spin-off effects for Europe's security and prosperity. Here, the EU and its Member States need to be prepared to operate in complex geopolitical settings that challenge our values-based external action, calling for principled pragmatism, both from a humanitarian and a broader geostrategic perspective.

→ Further reinforce the role of EU CSDP missions and operations and coordinated maritime presences to enhance mutual resilience, including to safeguard international shipping routes and critical infrastructures.

CSDP missions and operations contribute in various ways to building the capacities and resilience of their host countries, which in turn also helps to reinforce the EU's security at home. In line with mutual interests, the EU and Member States should further consider the use of CSDP missions and operations as a tool to ensure the security of key maritime routes, as shown already by EUNAVFOR ASPIDES in the Red Sea. In this context, innovative approaches could be developed to facilitate the use of CSDP instruments in complementarity with internal security tools in the immediate vicinity of the EU's territory or territorial waters, for example to protect critical energy infrastructure at sea or submarine cables, also in cooperation with close partners.

→ Develop an integrated EU approach to address the arc of instability and fragility in the EU's wider neighbourhood and tackle knock-on effects on European security and stability.

The widening and deepening belt of instability and fragility needs to be treated as a key issue of concern for the EU's preparedness. Fragile contexts are not only home to 73% of the world's extreme poor (2022), but also 29% of the world's disaster events (2019-2022), and 80% of all conflict-related deaths. In addition, fragile contexts generate the majority of the world's refugees and internally displaced persons. Three-quarters of the global refugee population have fled from fragile contexts[09].

In line with the principle of mutual resilience, addressing the issue of fragility is both a matter of value-based external action and of the EU's essential interests. In particular in the EU's wider neighbourhood, the widening arc of instability and fragility is not only eroding human, food, environmental, economic, and resource security, but also amplifying risks of negative spillovers and cascading effects. In addition, many fragile contexts stand increasingly at the forefront of geopolitical contestations and are often governed by regimes politically estranged from the EU, further complicating diplomatic, development and security engagement, including CSDP missions and operations.

09. OECD. States of Fragility. 2022.

Against this backdrop, ODA to fragile contexts decreased by over 10% from 2020 to 2022. The decrease in ODA was especially drastic in the most challenging contexts – extremely fragile settings, such as Sudan, Syria, the Democratic Republic of the Congo, Somalia, and Afghanistan[10]. While development and humanitarian funding cannot prevent or end conflict or instability, political and financing withdrawal can deepen fragility and insecurity, further eroding societal resilience and increasing the risk of knock-on effects for the EU, including growing push factors for irregular migration to Europe. At the same time, the EU faces the prospect of losing its previous investments, as well as any leverage and long-term opportunities to exercise positive influence.

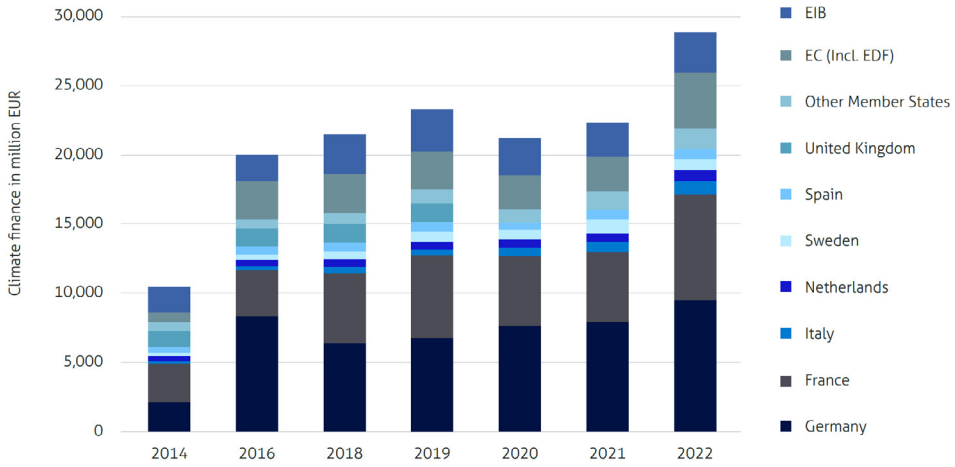
As part of an **integrated approach towards fragile and conflict-affected countries**, and in line with the Humanitarian-Development Peace Nexus, the EU should **develop dedicated financing instruments and a framework for pragmatic engagement in complex political environments**, working closely with Member States, International Financial Institutions, Multilateral Development Banks, and regional organisations. The aim should be to strike a balance between the need to stay engaged pragmatically, supporting local populations and avoiding giving support to unlawful or abusive ruling authorities. Such an integrated approach should not only promote stabilisation, but also address longer-term climate-induced hazards, basic needs, food insecurity, and social protection needs, tackling root causes of fragility and, where possible, build foundations for long-term resilience.

→ Ensure that international climate finance mechanisms are designed to reach the most climate-vulnerable countries and communities, and reinforce EU assistance to help address the growing consequences of conflict and disasters.

While climate change is increasing humanitarian needs everywhere, especially in fragile contexts where local communities are disproportionally affected by extreme weather-events and their consequences, international climate finance committed to fragile and conflict-affected settings remains significantly lower than allocations to other low-income countries. For instance, in 2020, countries experiencing high-intensity conflict received just USD 2.74 per capita in climate finance, and those experiencing medium-intensity conflict USD 5.06 per capita – less than two-thirds of the funding per capita received by other low-income countries[11]. This climate financing gap is growing. Increasing humanitarian needs are met with limited resources. Coordinated efforts are needed from the perspectives of development, peace-building, humanitarian, and climate action, including ensuring that more climate funds reach the most vulnerable countries and communities to strengthen their resilience and preparedness for disaster.

FIGURE 16

Team Europe + UK international climate finance contributions (2014-2022)



Source: Based on Climate Action Network (CAN) Europe, 2024.

10. OECD, INCAF Facts and Figures Series: ODA final data and trends for 2022 in relation to fragile and conflict-related contexts, 2024.

11. World Bank, Closing the Gap: Trends in Adaptation Finance in Fragile and Conflict-affected settings, 2024.

CHAPTER · CHAPTER · CHAPTER

09

Harnessing the economics of preparedness by investing together upfront

The EU's preparedness and readiness require upfront and consistent long-term investment. The logic of investing more, better and together as Europeans in these areas is the most effective way to address the increased and multifaceted risks we already face now and need to anticipate in the future. A well-prepared Europe will be more resilient to crises, better able to prevent them and faster in recovering from them. Smart and sufficient upfront investment in our preparedness is essential to minimise the cost of non-preparedness.

From a competitiveness perspective, Special Adviser Mario Draghi has already outlined the scale of the significant additional annual investments required to address climate, digital and defence-related challenges. This ties in with the preparedness dimension of these key risk drivers, **creating the potential to join up the EU's competitiveness and preparedness investments**. The daunting scale of the overall investment needs, moreover, means that Europe should harness the economic and strategic potential of these investments primarily to the benefit of the Union's economy and citizens – including their comprehensive preparedness.

In response to the economic consequences of the COVID-19 pandemic, exacerbated by the economic fall-out of Russia's aggression against Ukraine, the EU has devoted major resources to support Member States' recovery and make their economies and societies more resilient and better prepared for the future. This not only reflects the enormous impact that a major crisis - or confluence of crises - can have on Europe but also the financial capacity needed both to be better prepared and manage the economic consequences. With the Recovery and Resilience Facility, the EU set up an unprecedented debt-based instrument composed of non-repayable and repayable support (close to EUR 650 billion in total) to support reforms and investments in Member States to this end.

Moreover, the EU has also allocated EUR 23.2 billion to external crisis management in the wider sense[01] and EUR 3.6 billion for the UCPM and the rescEU strategic reserve. However, the need to **fund ad**

01. This includes humanitarian aid funding, the NDICI Response Pillar, EU aid volunteers under the European Solidarity Corps, and CSDP missions under the CFSP.

hoc response measures has led to a partial repurposing of funds allocated to preparedness and other long-term initiatives. Moreover, while the creation of Next Generation EU (NGEU) has provided much-needed relief to an already over-leveraged MFF, its 'one-off' nature also raises questions regarding not only the possible scale-up, but even the long-term financing security of core initiatives, such as the rescEU strategic reserve, which has been reinforced with NGEU top-ups during the pandemic. Despite the drastic deterioration of Europe's security situation following Russia's full-scale invasion of Ukraine in 2022, there was **only a small increase in security and defence-related funds within the EU budget**.

While the 2024 mid-term revision of the MFF did result in a sizeable new long-term funding facility to support Ukraine, only EUR 1.5 billion was made available to fund the EU's defence industrial scale-up under the new European Defence Industrial Programme (EDIP). With EUR 14.5 billion, the MFF's overall Security and Defence heading – created for the first time in 2019 – also remains relatively modest. The funds for military mobility have already been exhausted. The current level of funds does not match the scale of additional investment needed to meet the demands of better preparedness for our own deterrence, as well as to support Ukraine in the long term, as explained in chapter 7 of this report. In fact, against the backdrop of the strategic context and the identified capability needs, the Commission has assessed that additional defence investment of around EUR 500 billion is needed over the next decade[02].

Seen through a preparedness lens, the overall structure of the EU's budget still remains too fragmented in some areas, limiting our ability to optimise the use of our funds and to invest in cross-sectoral priorities. The differences and divisions between the EU's financing instruments – each coming with their specific requirements and funding criteria within specific sectors – make it challenging to mobilise funding at scale for projects of common interest that serve cross-sectoral priorities and multiple (dual-use) use cases – for example, in relation to critical infrastructure. Instead, the fragmentation of our instruments may often result in funding to several, partially overlapping, small-scale projects, without harnessing the full potential of its scale.

Setting aside difficult political discussions about relative sectoral priorities, **investing together in our own security and safety is one of the primary responsibilities the Union faces in an era of high risk and deep uncertainty**. Shocks, disruptions and crises of Union-wide scale and impact require a level of coherent investment and oversight that need to be enshrined in an EU framework. To address these challenges and make the most efficient use of their budgetary resources, the EU and Member States should approach the design of the next EU budget from a preparedness logic, embracing 'preparedness-by-design' as a guiding principle cutting across different dimensions.

The following **interlocking guidelines** should provide a starting point in this regard:

→ Preparedness for the high-risk context of the coming years and decades requires scaling up our joint investment across the board to a new level.

For instance, beyond the required additional defence investment mentioned above, the estimated cost for climate change adaptation may range from EUR 15 billion (lower bound) to EUR 64 billion (upper bound) until 2030[03]. Given the scale of the challenges, which exceed Member States' capacity to act singlehandedly, there is a clear need for coordinated EU action. Measures to strengthen preparedness in line with recommendations of this report all require adequate funding, reinforced accordingly, to keep pace with the growing scale of the challenges, risks and threats. **Communicating clearly and publicly about these risks and the aim of comprehensive preparedness to keep Europeans secure is important to generate the necessary political and public support for prioritising higher investment levels**. This is necessary to identify the most important needs and the most efficient ways of enhancing preparedness to meet them.

02. European Commission, Opening remarks by President von der Leyen at the joint press conference with President Michel and Belgian President De Croo – EUCO of June 2024, 2024.

03. The World Bank, Climate Adaptation Costing in a Changing World, 2024.

An elemental part of budgetary preparation and decision-making must be to identify clearly where EU-level investment and action are the most impactful and strategic and provide opportunities that are not available to Member States with only national resources. Breaking down stovepipes and expanding defence-related or dual-use expenditures would unlock greater synergies and efficiencies.

→ Preparedness comes at a cost – but its economic rationale is strong.

It reduces risks, can prevent a crisis from erupting, mitigates its consequences and limits damage, and enables recovery to kick in much faster. If a serious threat does materialise, the cost of non-preparedness may become astronomically higher than the investment required upfront. In view of ever more frequent weather extremes and global trade disruptions, the cost of inaction is set to increase even further. For instance, between 1980 and 2022, weather and climate-related extreme events have affected millions of people in the EU and have cost Member States EUR 650 billion in total – EUR 112 billion of which only between 2021-2022[04]. Along similar lines, the macroeconomic cost of the COVID-19 pandemic for the Eurozone is estimated at 16% of GDP (2019 level) between 2020 and 2021[05].

While no preparedness measure can fully prevent the next pandemic, having at hand the right resources and focusing them on the most strategic needs from the outset is crucial for limiting damages, most importantly in human terms, but also economically. Upfront investment is essential to shifting gear and moving beyond a reactive approach to crisis management. **Investing in disaster-resilient and climate-adapted critical infrastructure, building up stockpiles of critical goods and financially supporting businesses engaging in supply chain diversification can help the EU to enhance its capacity to absorb shocks and provide a boost to the EU's economy in the process**.

The World Bank and the European Commission have undertaken extensive work to quantify the economic benefits of investing in prevention and preparedness. For instance, EUR 1 invested in pandemic preparedness can generate average returns of EUR 13.3. Investing in all-hazards early warning systems pays off as well. For heatwave early warning systems, the return on investment reaches on average EUR 130 for each EUR 1 invested[06]. Similarly, a higher level of defence readiness helps to deter aggression. Even a limited form of external armed aggression on our territory would have devastating social, economic, and political consequences throughout Europe – without considering the immediate human cost and broader security consequences. Investing more and smarter in Europe's defence readiness is also necessary to maintain our support for Ukraine's ability to defend itself in the long term, which is a precondition for any just peace that could last and prevent further Russian aggression.

Realistically, it is of course not possible to reach a state of preparedness that fully covers each and every eventuality, anticipates all possible cross-sectoral cascading effects or prevents any impact on the general economic outlook (consumer confidence, etc). **Achieving a higher overall preparedness baseline, however, does enable the economy and society to bounce back faster** when a new pandemic, a major disruption, disaster or crisis hits the EU, including by protecting the most vulnerable. In addition, a demonstrated commitment to preparedness at the governmental level has a crucial impact on mindsets, permeating society by reinforcing public trust in government and generating confidence among investors and citizens.

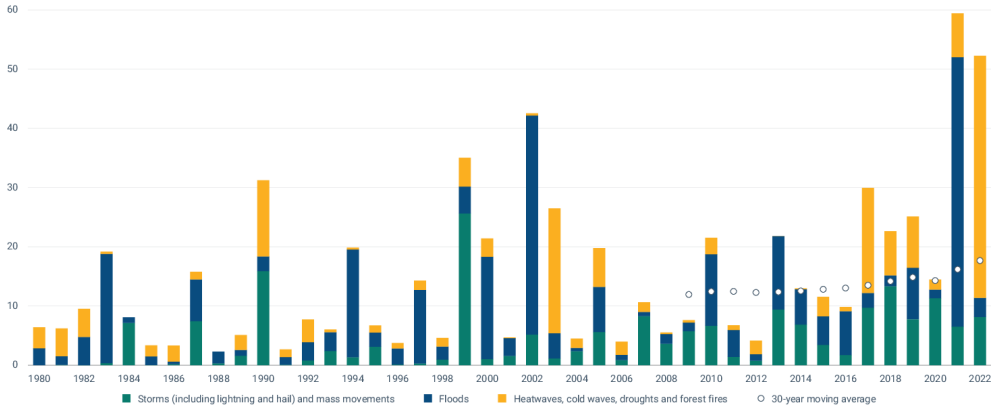
04. European Environment Agency, Economic losses from weather- and climate-related extremes in Europe, 2024.

05. González López-Valcárel, B., and Vallejo-Torres, L., The costs of COVID-19 and the cost-effectiveness of testing, 2021.

06. World Bank and European Commission, Economics for Disaster Prevention and Preparedness: Financial Risk and Opportunities to Build Resilience in Europe, 2021.

FIGURE 17

Annual economic losses caused by weather and climate-related extreme events in EU Member States (EUR billion in 2022 prices).



Source: European Environment Agency, 2024.

→ Robustly investing in preparedness at the EU level means ensuring that our efforts are effective, coherent, cost-efficient, and mutually reinforcing.

Moreover, it is also an expression of solidarity and interdependency among Europeans, making sure that no single Member State has to shoulder costs that are otherwise too great to bear. It contributes to the further integration of the Single Market and the competitiveness of EU industry. Disjointed national efforts that fail to seize on economies of scale are no longer tenable from a European perspective. Instead, the economic rationale of preparing together at the EU level is exemplified by the joint purchases and pooling and sharing of resources that are needed in disasters, but which do not make sense for all Member States to acquire nationally.

The rescEU firefighting fleet that is financed with EU support has already proven its value in providing the reserve of planes and helicopters that can be used in Member States hit by forest fires. The lessons from the COVID-19 pandemic and Russia's invasion of Ukraine have shown that we need to closely coordinate the procurement of crisis-relevant goods, negotiating as a single buyer with critical suppliers and making sure that all Member States have access to limited industrial capacity without driving up prices too much. The need to increase preparedness against the manifold risks to our security at a time of slow economic growth, increasingly finite resources and competing domestic spending priorities, underline the importance of cooperating more structurally. This applies both in terms of preparedness, for example through coordinated stockpiling efforts [see chapter 5], and when a crisis hits, for instance by expanding procedures for joint purchasing in emergencies or emergency derogations from public procurement rules.

→ Integrating preparedness-by-design into the EU's next multi-annual budget starting in 2028 will require strengthening both short-term flexibility and coherence with long-term priorities.

× **Addressing fragmentation in the EU budget will be important to ensure sufficient built-in flexibility to respond to unforeseen events and emergencies**. Recent years have shown that sudden disruptions can raise new demands and create significant burden for the EU's financing instruments. Be it in the field of energy, health, civil protection, or defence, short-term crisis response measures, purchases, and investments can be necessary to alleviate immediate pressure. The EU and Member States' ad hoc efforts to support the rapid development of COVID-19 vaccines, to build new LNG terminals, and procure military equipment are prime examples in this regard. Emergency reserves should be bolstered and budgetary instruments should enable the redirection and pooling of funds without creating unnecessary delays in preparing for and reacting to emerging needs.

- **At the same time, we need to ensure consistency with our long-term policy objectives, even when addressing short term urgencies**. Ad-hoc crisis response measures and related investments should ideally be limited in time and scope. They should also, where possible, be combined with longer-term measures to avoid deviating from our strategic and long-term objectives, whether related to climate change mitigation or strengthening European defence capabilities.

→ Preparedness investments can be a boost for enhanced European competitiveness in a rapidly changing global economy.

We can and need to design our investment in such a way that it generates European added value in terms of competitiveness, industrial capacity, jobs and innovation. Currently, certain critical investments – both within the defence sector and other fields relevant for preparedness – are often made outside of Europe, for different legitimate reasons. However, this ultimately undermines the necessary scale-up of industrial capacity in these sectors at home.

We need to reverse course and use preparedness investments to boost our industrial and technological competitiveness – which also contributes to the EU's long-term preparedness and crisis resilience. For instance, regarding the protection and integrity of communication and information systems, and of related supply chains, the EU can require the application of specific conditions when awarding Union funds linked to strategic assets and interests, such as digital and space infrastructure to ensure – in line with Article 136 of the recently revised Financial Regulation – the EU's essential security interests[07].

We must also be ready to invest in reducing and removing existing vulnerabilities so as to replace, for example, high-risk components from critical networks or to ensure that at least a controlling stake of ownership in strategically critical EU-based companies is in trusted hands. In addition, EU funds should be used to ensure that sufficient quantities of critical commodities for different crises are produced within the EU to avoid the risks associated with extensive reliance on external suppliers.

07. Regulation (EU, Euratom) 2024/2509 on the financial rules applicable to the general budget of the Union (recast).

Recommendations

1. Integrate preparedness by design in the next EU budget:

- × Ensure more built-in flexibility in the next MFF.
- × Reinforce the long-term 'preparedness impact' of EU investment and, in particular, crisis recovery spending.
- × Adapt the EU's budgetary framework to better support multi-year funding and investment, and to secure the long-term financing of key preparedness investment.
- × Ring-fence funding for preparedness action.
- × Strengthen the dual-use potential of our spending.

2. Consider a European Preparedness and Readiness Investment Framework, providing details on the EU's transition to a fully prepared Union:

- × Establish an Investment Guarantee Programme to trigger investment in Europe's defence technological industrial base.
- × Work with the European Investment Bank to expand funding possibilities for the defence sector beyond dual-use.
- × Leverage private capital for preparedness action by providing investment opportunities for EU citizens' savings.
- × Leverage the synergies between the EU's work on competitiveness and preparedness.

1. INTEGRATE PREPAREDNESS BY DESIGN IN THE NEXT EU BUDGET:

With a view to the preparation of and negotiations on the next MFF, and taking into account the increasing risks in the EU's security environment, preparedness should be integrated by design in the EU budget. This means addressing the fragmentation of funding instruments, enhancing short-term flexibility and strengthening options for pooling funds in line with overarching priorities. This is necessary to ensure that the next MFF will fully support the long-term preparedness objectives of the EU. In line with this, we should:

→ Ensure more built-in flexibility in the next MFF.

To allow for a faster and more effective response to unforeseen needs that arise in the wake of emergencies and crises, EU budgetary frameworks and decision-making need to have sufficient flexibility. Important steps were already taken as part of the recent mid-term review of the MFF, which led to a strengthening of the Solidarity and Emergency Aid Reserve (SEAR), as well as the creation of a financial reserve of EUR 450 million a year to mitigate the impact of crises on the food sector. Nevertheless, reflecting the growing scale of our challenges, the EU and Member States need to further strengthen scalable, fast-deployable and all-hazards EU financial mechanisms and instruments.

Flexibility mechanisms should account for both smaller-scale disasters and emergencies, for instance by strengthening emergency reserves, and for the severe impact of major unforeseen

cross-border crises (e.g. COVID-19), for instance by putting in place a 'force majeure' process that could include specific triggers to activate scaled-up crisis response budgets, and other crisis procedures in existing instruments and mechanisms. This would also address the challenge of EU-level trigger mechanisms efficiently allocating funds in the event of crises and disasters remaining underdeveloped.

→ Reinforce the long-term 'preparedness impact' of EU investment and crisis recovery spending.

All major structural and regional investment supported by the EU budget should have security risk and disaster-proofing, climate-resilience and crisis-preparedness components further integrated by design. Different funds and policies should complement and mutually reinforce each other throughout the crisis and disaster management cycle – in particular, in the context of recovery – and adopting a more strategic and impactful policy-based approach. A concrete example could be to review the European Solidarity Fund[08] to ensure that when Member States build back from a major disaster by nationally drawing on EU funds, at least 15% is invested in disaster risk reduction or other peer-assessed preparedness measures. Recovery from disasters and other emergencies provides a key opportunity to invest in building back better and strengthening preparedness measures. The EU Solidarity Fund should be conditioned on inclusion of specific crisis preparedness and disaster prevention measures.

→ Adapt the EU's budgetary framework to better support multi-year funding and investment, and secure the long-term financing of key preparedness investment.

The EU and Member States need to make sure to offer public and private partners the necessary investment horizon, and to secure a long-term commitment to preparedness initiatives. Depending on the sector, co-legislators have at times insisted on annual work programmes that hamper a more strategic and longer term stream of investment. In other cases, funding can only be guaranteed on a year-by-year basis in line with the EU's financial rules. Securing the long-term financing necessary to further develop and maintain key preparedness investments, such as the build-up of strategic stockpiles and response capacities under rescEU, which was largely financed under 'one-off' funding, should be another priority.

→ Ring-fence funding for preparedness action.

To ensure that responding to the needs of an immediate crisis does not hamper our long-term efforts, response costs must not come at the detriment of further prevention and preparedness action. In particular, in the context of civil protection, and to some extent in other sectors, increasing response needs often leads to a situation where funding for preparedness action, such as training, exercising and cross-border capacity building, is increasingly depleted. Response action tends to be reinforced through emergency reserves, which is not usually the case for preparedness action.

→ Strengthen the dual-use potential of our spending,

fully exploiting possibilities under the Treaties and applicable regulatory frameworks to ensure we maximise funding benefits and added value for our civilian and military readiness – as set out throughout this report.

08. The EU Solidarity Fund provides EU budgetary support to individual Member States to recover from the aftermath of disasters.

2. DEVELOP A EUROPEAN PREPAREDNESS AND READINESS INVESTMENT FRAMEWORK TO SUPPORT THE EU'S TRANSITION TO A FULLY PREPARED UNION:

As part of such an investment framework to be envisioned for the next multi-annual budget, the EU should bring together relevant instruments in a coherent package with funding levels commensurate to the scale and complexity of the evolving challenges we face. On the one hand, in line with the notion of integrating preparedness by design, all relevant instruments across sectors should earmark a certain amount for preparedness action in their respective fields – so that for example at least 20% of the overall EU budget contributes to EU security and crisis preparedness.

On the other, the EU and Member States should consider setting up two dedicated facilities – the **Defending Europe Facility (DEF), and the Securing Europe Facility (SEF)**, combining relevant funding streams and avoiding fragmented, siloed instruments. The creation of two large-scale facilities with relevant windows for different activities should facilitate the pooling of resources, enabling the EU to better leverage its funds at scale for common and overarching priorities, simplifying public and private partners' access to EU-funded programmes, and contributing to EU competitiveness by boosting market consolidation.

- The **Defending Europe Facility** should encompass relevant defence industrial and other defence-related or dual-use instruments. The DEF should support EU's defence industrial capacity, common procurement, dual-use research, development and innovation, including for developing new defence applications and capabilities, and scaling up existing infrastructure and human-capital-related initiatives in this area.

- The **Securing Europe Facility** should combine all instruments and programmes linked to civil security (e.g. law enforcement and border management), civil protection, and other emergency response services, and related critical infrastructures. In particular, the SEF should strengthen the connection between EU funding for civil security R&I and financial support for the further operationalisation and deployment of innovative solutions. Currently, there is an insufficient connection of civil security research from development to deployment, and joint cross-border procurement. Many innovative ideas remain at the prototype level, rather than being scaled-up further. In this vein, the SEF should jump-start a much-needed capability-driven approach to civil security, from the definition of key capabilities and the identification of gaps and needs, to research and deployment. This requires stronger structural links between funding instruments across the research-innovation-deployment continuum.

As part of this comprehensive **European Preparedness and Readiness Investment Framework**, the EU and Member States should explore further creative and innovative ways to mobilise the necessary funding for preparedness:

→ Establish an Investment Guarantee Programme,

e.g. on the model of InvestEU, to trigger private sector investment in Europe's defence technological and industrial base or disaster and crisis-resilient infrastructure through public seed money.

→ Work with the European Investment Bank to expand funding possibilities for the defence sector beyond dual-use.

The EIB has recently agreed to an expanded definition of dual use, but still has constraints with regard to the direct funding of the development of defence products in view of preserving its financial capacity and credit rating. However, given the defence industry's vital role for the EU's security, further steps should be taken to reduce these constraints as part of a broader effort to mainstream investment in the defence industry under the ESG taxonomy.

→ Leverage private capital for preparedness action by providing investment opportunities for EU citizens and institutional investors.

For instance, the European Commission and the European Investment Bank could:

- Issue a '**European Preparedness Bond Standard**' on the model of the European Green Bond Standard used to finance assets or economic activities needed for the low-carbon transition. Along these lines, a dedicated voluntary standard defining economic activities critical for preparedness could help to steer private investment to sectors or companies critical for preparedness and encourage companies seeking certification to comply with heightened resilience measures, including in relation to supply chain diversification.

- Encourage EU-based financial institutions to create a series of **preparedness-themed Exchange Traded Funds (ETF)** targeting EU companies in crisis-relevant sectors, and support their uptake through proactive communication. For instance, this could include defence technology and manufacturing, cybersecurity and intelligence-related technologies, health and medical supplies, companies producing goods relevant for emergency response (e.g. shelter), or companies investing in secure supply chains for critical goods. Such thematic ETFs could provide EU citizens and investors with easily accessible investment opportunities, while also contributing to enhancing the EU's resilience and preparedness.

- Encourage private stock companies to consider the creation of **EU-level thematic stock indices focusing on companies involved in civil and military preparedness**. For example, an EU Defence and Security Index, including companies across Europe that are key players in defence contracting, or a Critical Infrastructure Resilience Index, focusing on critical companies in sectors, such as utilities, telecommunications, energy and transport, could provide investors with a consolidated EU-level overview.

→ Leverage the synergies between the EU's work on competitiveness and preparedness.

For instance, the future EU Competitiveness Fund announced in the Political Guidelines (2024-2029) will provide an investment capacity to support strategic sectors critical to the EU's competitiveness and will be targeted towards the needs of the EU's economies and businesses. It could, for example incentivise to EU companies and economic operators to address vulnerabilities in their infrastructure or supply chains [see also recommendation 2 in chapter 5]. Specifically, the Competitiveness Fund could provide investment support for re-shoring production, diversifying supply chains, or replacing potentially untrustworthy components in their networks.