ISSUE

REPORT Nº 34 — June 2017

What if ...
Conceivable crises: unpredictable in 2017, unmanageable in 2020?

EDITED BY
Florence Gaub

Reports

ISS European Union Institute for Security Studies

EU Institute for Security Studies

100, avenue de Suffren

75015 Paris

http://www.iss.europa.eu

Director: Antonio Missiroli

© EU Institute for Security Studies, 2017.

Reproduction is authorised, provided the source is acknowledged, save where otherwise stated.

PRINT ISBN 978-92-9198-624-8 ISSN 1830-9747 doi:10.2815/531911 QN-AF-17-005-EN-C

PDF ISBN 978-92-9198-625-5 ISSN 2363-264X doi:10.2815/31849 QN-AF-17-005-EN-N

Published by the EU Institute for Security Studies and printed in France by Jouve.

Graphic design by Metropolis, Lisbon.

Cover photograph credit: © WIREPEC/ADOBESTOCK

CONTENTS

Foreword 3

Antonio Missiroli

Introduction – Our approach 5

Florence Gaub and Daniel Fiott

I. What if … Daesh attacks a cruise liner in the Mediterranean? 13

Florence Gaub

II. What if … Russia intervenes again in Ukraine? 17

Daniel Fiott

III. What if … Israel and Hizbullah fight another war? 21

Julia Lisiecka

IV. What if … Bosnia-Herzegovina disintegrates? 25

Zoran Nechev

V. What if … Europe is struck by right-wing terrorism? 29

Annelies Pauwels

VI. What if … the US misreads Turkey? 33

Roderick Parkes

VII. What if … Daesh seizes an African country? 37

Julia Lisiecka and Aleksandra Tor

VIII. What if … a coup is launched in Cameroon? 41

Aleksandra Tor and Alice Vervaeke

IX. What if … North Korea invades South Korea in cyberspace? 45

Patryk Pawlak

X. What if ... Japan goes nuclear? 49
Eva Pejsova

XI. What if ... conflict erupts between India and Pakistan? 53
John-Joseph Wilkins

Annex 57

FOREWORD

Antonio Missiroli

In a world increasingly shaped by unexpected events and developments – ranging from 'strategic surprises' like 9/11 or the Arab Spring to the unintended consequences of often well-meant decisions – trying to imagine contingencies that challenge current assumptions may well prove a useful exercise. Imagination should not be stretched too far though, or else the resulting scenarios would lose plausibility. These need to build upon at least some already available evidence, to develop that into less consequential situations, and to push people out of their mental and operational comfort zone. The main contribution of such an exercise would thus be to raise awareness and potentially preparedness among policymakers – be they planners or first respondents – and to prevent complacency and 'groupthink'.

When the EUISS team began considering engaging in this effort, the first common approach that was discussed was a 'What if … ?' question. The 'What if' label has been often associated with counterfactual situations linked to a different historical past and its possible consequences – starting with works of fiction (such as Philip K. Dick's *The Man in the High Castle* and Robert Harris' *Fatherland*, both depicting an alternative outcome of the Second World War) and ending with exercises in 'virtual history' (as coordinated by Niall Ferguson or Robert Cowley) and visions of 'altered pasts' (as conceptualised by Richard Evans). In a similar vein, the weekly newspaper *The Economist* has published a series of scenarios built on *The World If*, combining virtual futures, alternative pasts and various hypothetical situations in business, science and politics.

Another approach adopted more recently, which is more pertinent in terms of foresight and risk analysis, is related to the identification of so-called 'grey swans', i.e. contingencies that are less unpredictable than the highly improbable 'black swans' famously described by Nassim Nicholas Taleb in early 2007, but still in the realm of the unexpected, unforeseen and unplanned for: the events that unfolded in Ukraine in 2014 gave a boost to this particular approach, which translated, *inter alia*, into a series of publications by the Berlin-based Stiftung Wissenschaft und Politik (SWP).

The selection of scenarios collected in this report – coordinated by Florence Gaub in cooperation with Daniel Fiott and John-Joseph Wilkins – tries to combine those two main approaches by focusing exclusively on critical developments (possible dark storms erupting into relatively clear skies) and by imagining them as having already materialised, with an emphasis on how much worse they can still turn in the near future and how avoidable they could have been in the recent past. While they inevitably display different shades of grey and different blends of fact and fiction, they all straddle the

same three time zones – not unlike the well-known 'Back to the Future' film trilogy, but with shorter intervals than the 30-year time warps of the movies (the methodology is explained in more detail in the introduction). They also cover a wide variety of geographical and operational situations while never explicitly calling into question specific EU actions or policies – only general EU principles and interests. The overall intent of the exercise and resulting report is not to divine future crises – actually, and paradoxically, the authors would be delighted to be proven wrong – but to stimulate creative thinking and clever planning while offering a good read.

INTRODUCTION – OUR APPROACH

Daniel Fiott and Florence Gaub

There is no doubt that we live in a time of political upheaval and uncertainty, but all too often our ability to think about possible future trends and shocks can give way to the pressing needs of the present. Especially in times of severe crisis, the temptation can be to focus on the present or near future. What will happen to migration flows *this summer*? Could that missile launch occur *this week*? Will the election *next month* fall victim to an external disinformation campaign? How will the oil markets fare *today*? The pressures associated with devising policy responses to crises that are in motion *now* may detract from the ability to think about *what may come* – the future.

Yet it is worth thinking about the consequences of neglecting longer-term political dynamics. This is especially true when it is considered that crises are rarely isolated phenomena. As history and experience show, one crisis can bleed into another. Single crisis events are usually symptoms of longer-term social, technological, economic, environmental and political (STEEP) trends that affect the world as a whole. Events are usually the dots that connect trend lines, although sometimes crises may seemingly emerge out of the blue. It is also important to bear in mind that crises occurring over a longer period of time may not necessarily respect borders. Planning for – or at least thinking about – future crises is thus a cross-cutting temporal and geographical endeavour.

The EU Global Strategy (EUGS) is correct to refer to a 'world of predictable unpredictability' and the intention of this report is *not* to predict the future. In any case, it would be necessary to think about a range of events possibly occurring – not one *future* but a spectrum of *futures*. It is true that a range of sophisticated data gathering systems ('big data' and 'deep data') can help analysts detect trends and the probability of an event occurring in the future in ways certainly not foreseen (even) by Nostradamus. The purpose of this report is not to predict a single or set of futures. In this report there is therefore no attempt to devise probability scales, complex algorithms or to use traditional foresight techniques such as SWOT (Strengths, Weaknesses, Opportunities, Threats) or PESTLE (Political, Economic, Social, Technological, Legal, Environmental) analyses.

Grey swans, red teams and back-casting

There remains a desire to think about possible future events and scenarios because it may help us to recalibrate the crisis management systems we have today. Risk is an important feature of political and economic life, and so the impulse to detect and prepare for surprises is strong and understandable. Sometimes this can be difficult: the 9/11

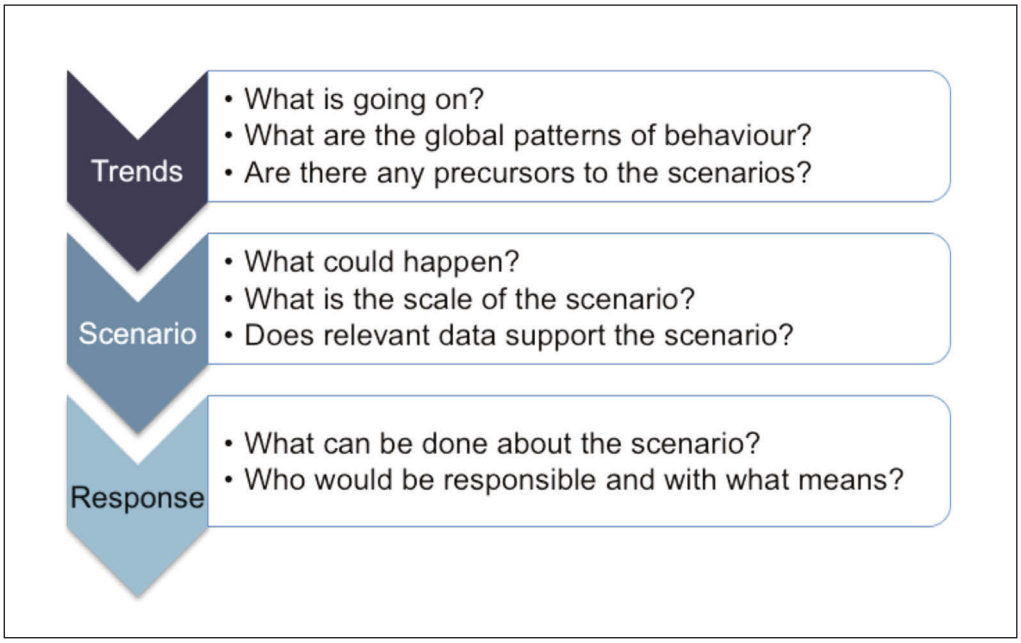
terror attacks and the 2008 financial crisis are just two cases in point. However, without a combination of scientific analysis, intelligence and strategic foresight would it have been possible to avert the ozone layer crisis after the 1980s, eradicate malaria in parts of Europe from the 1940s and/or avoid the 1962 Cuban missile crisis? The probability of a political, economic or strategic event occurring in the future has been famously likened to the chances of seeing black, grey or white swans. 'White swans' are those events that are relatively predictable in nature (e.g. an earthquake occurring in a high-risk seismic area). 'Black swans' are events that are extremely unlikely to happen (e.g. an alien attack on planet earth). However, 'grey swans' refer to events that may seem unlikely now but which could happen at one point in time (e.g. any of the scenarios contained in this report).

The grey swan scenarios presented in this report are designed to tell a number of stories to help decision-makers think about possible responses to crises and how they can be prevented. The focus should not be on the scenario *per se*, but on what the scenario tells us about the vulnerabilities and strengths that lie in existing decision-making processes and crisis management structures. Such vulnerabilities and strengths are as much about our intellectual ability to grapple with a crisis situation as the practical or material responses. Therefore, strategic foresight and scenario-building may help us challenge ingrained ways of thinking about how we would deal with a range of grey swan situations. In this sense, Warren Buffett was partly right when he stated that 'forecasts may tell you a great deal about the forecaster; they tell you nothing about the future'. The point about the kind of grey swan scenarios found in this report is that they can help challenge existing intellectual, institutional and/or material responses to crises. They can also help us think about how crises may be prevented or averted. When reading this report the immediate question that should come to mind is not 'could that really happen?' but rather 'would we be prepared to deal with it if it did occur?'.

Each contributor in this report has put themselves in the shoes of an adversary, partner and/or ally and the scenarios have been developed on this basis. For those familiar with strategic foresight exercises, the scenarios in this report follow the logic of 'backcasting'. This is where decision-makers can follow the sequence of events by working backwards from some future date to the present period. In doing so, the aim has not been to pass judgement on whether policymakers have made good or bad decisions in the past – although potential policy failures will be apparent when reading the scenarios in this report. Instead, this report generates scenarios in the hope that they will serve as a mirror for decision-makers and crisis managers; one that allows these individuals to think about their own approaches to potential grey swan scenarios and the crisis management architecture that is currently in place.

Anyone familiar with the idea of 'red teaming' and 'blue teaming' will understand the approach taken in this report. 'Red teaming' refers to an exercise where an independent team of people tests the vulnerability, readiness and effectiveness of their own organisation – they essentially play the role of devil's advocate. 'Blue teaming' is where an independent team within the same organisation tries to fend off the manoeuvres and strategies of the 'red team'. In each scenario presented in this report, EUISS analysts play the role of the 'red team' and decision-makers are invited to join in the 'blue team'.

FIGURE 1: METHODOLOGY



Fact, fiction and bias

The scenarios outlined in this report share some baseline criteria. First, the scenarios must allow for a prevention strategy and/or crisis management response and therefore avoid 'ground zero' scenarios such as nuclear war. Second, they must affect the security of Europe in some way. Such scenarios are defined in a relatively broad way, but each one should be significant enough for European policymakers to need or least want to respond. Third, it should be possible to build up a quantitative and qualitative picture of the specific trigger event or shock selected. If there is little to no data or sources on which to build a convincing case for why a grey swan scenario might occur, then the scenario should be dropped. Fourth, each scenario must be submitted for peer-review by fellow analysts at the EUISS and select experts from outside the Institute. Prior to the publication of this report, several internal meetings and exchanges and expert workshops were organised to test the salience of each scenario. Finally, each scenario should be time-limited in nature – the aim is not to describe shocks that could occur out to 2045 or beyond. The scenarios begin in 2018 and end at some point before 2025. This time period of approximately five years has been selected because it is aligned to electoral terms and the tenure of most senior officials.

In terms of the structure of the individual contributions in this report, analysts have followed the same stylistic and methodological approach when elaborating each grey swan scenario (see Figure 1 above). In terms of methodology, analysts have invested time into thinking about current and future STEEP trends and precursors (such as isolated events and/or actors). The report therefore acknowledges trends such as the rise of Daesh, Russia's resurgence, technological and health developments, etc. Once the trends have been established, the analyst moves on to thinking about possible scenarios that could be triggered out of these trends. When developing the scenarios, the analyst takes stock of past events (e.g. how many armed attacks have occurred, where intervention takes place, etc.) and then consults a range of data sources to craft a situational context that is as much a reflection of reality as possible. For example, many of the economic indicators used in the contributions derive from a range of reputable databases and the geographical names of places and regions used are not always fictitious. Although the trigger event in each grey swan scenario is thought-out in the context of trends and available data, the individual contributors are responsible for the specificities of each event. This report does not elaborate any responses – this is a task for the 'blue teamers' reading this report (see annex for a preliminary map of the EU's 'blue teams').

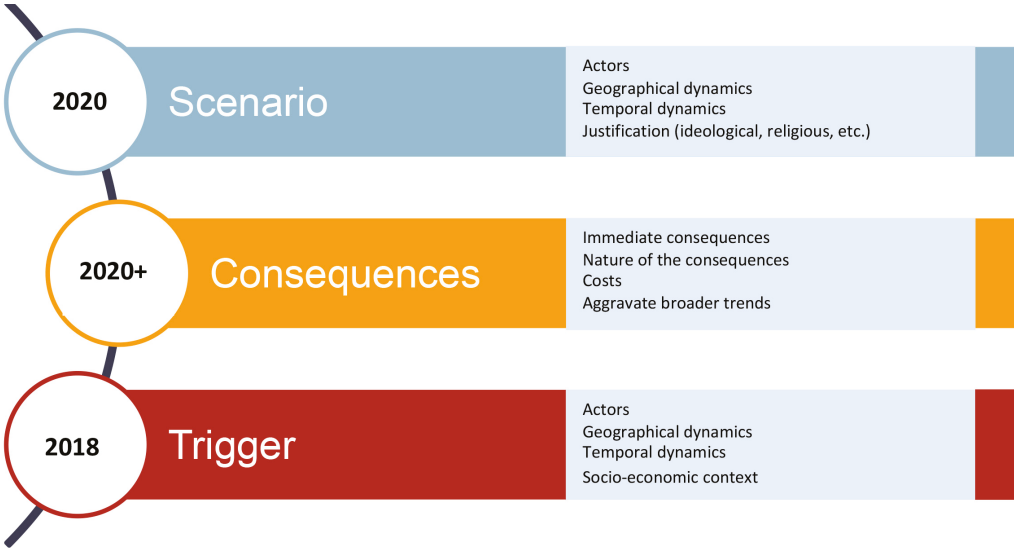
Whenever a strategic foresight exercise of this kind is undertaken, it is inevitable that questions about how each author balances fact and fiction and deals with bias arise. As stated, whenever possible each author has relied on data that is available today from a range of reputable data bases, media sources, think tank reports and open intelligence sources. However, facts often become quasi-irrelevant when thinking about the future. The whole point about generating a future scenario is that imagination trumps reality – in fact, an over-reliance on present-day data may even hinder the ability to think about future trends and surprises. As with strategy more broadly, strategic foresight is part science, part art. In balancing fact and fiction, this report ultimately takes a pragmatic approach. This report therefore engages in a hybrid mix of fact and fiction.

Bias is also an issue of debate when conducting strategic foresight exercises. 'Bias' here means the perceptions and assumptions an author brings to a scenario rather than a wilful manipulation or omission of data. Indeed, individual authors will inevitably colour each scenario with his or her cognitive assumptions about the world. Yet bias is an essential part of the enterprise of strategic foresight exercises. If as a reader you detect bias in one or more of the scenarios then this should ideally feed into crisis prevention and response planning. The bias of the 'red team' should not be discounted altogether. Bias may indeed be reflective of broader cognitive bias in the crisis prevention and response system – bias may serve as a strategic blind spot. It is, however, better to grapple with bias in the scenario foresight stage than during real life crisis situations.

The detection of bias should not lead to an accusatory stance. Engagement with the bias of an author may have self-critiquing qualities. Therefore, perhaps when bias is

detected the readers' immediate question should be 'what does a particular form of bias tell us about our crisis prevention or response system' rather than 'this scenario is biased, so disregard it'. The reader may use the issue of facts and bias as a way to discredit a scenario, but this may reveal more about the reader than the author. To discredit a scenario may lead to a 'dirty-white swan' scenario – i.e. wilful ignorance of an event that later becomes a 'surprise' event.

FIGURE 2: 'BACK TO THE FUTURE'



In terms of the structure of this report, each scenario first outlines the immediate effects of the trigger event (see Figure 2 above). This is followed by the broader political and strategic consequences of the trigger event, and finally the trigger event itself is described. Although the technical term for the methodology used in this report is back-casting, perhaps it is easier to draw on the medium of film to better understand the approach. Indeed, anyone familiar with the 'Back to the Future' film series will recognise our structure and approach. Each scenario begins in 2020; the year in which the major effects of the trigger event are felt. The scenario then moves onto a second phase focused on the 2020+ period; whereby the ripple effects of the trigger event materialise. Finally, each scenario travels back into the past to 2018 when the trigger event occurs. Each scenario therefore revolves around a similar time-scale: two years from the trigger event to the immediate consequences, and several more years for the full effects of the crisis to evolve.

Know your client ...

This is not the first time that EUISS analysts have engaged in strategic foresight exercises. In February 2015, the EUISS released a report entitled 'Arab futures: three scenarios for 2025'. In March 2016, the Institute built on this experience with a report on 'Russian futures: horizon 2025' and a Chaillot Paper on possible futures for European defence. In each of these reports and papers an emphasis was placed not on *prediction* but, as the Arab Futures report states, on '*possible*, *plausible*, *probable* and *preferable* futures'. These publications sought to outline a series of possible futures that could materialise based on mega trends that are currently underway. Yet these past exercises were geared to describing larger political and strategic dynamics that could occur in a particular region and/or policy area. In this report we focus on single specific shocks rather than trends. We purposefully do not offer the reader a multitude of potential scenarios so as to limit choice; a single scenario or outcome forces 'blue team' members to grapple with a crisis head-on rather than to debate what scenario is more likely to occur. Identifying specific grey swans that could disrupt Europe's security is a new exercise for EUISS analysts, but one which has helped to develop the Institute's strategic foresight skills. The scenarios contained in this report may well serve as a preliminary phase in a broader strategic exercise that could potentially lead to crisis management exercises and simulations.

All successful strategic foresight exercises rest on buy-in from relevant stakeholders. As stated, in this report the EUISS has assumed the role of the 'red team' but the project team have actively reached out to the 'blue team' for their feedback and engagement. Strategic foresight exercises are not of much use if they do not trigger debate and reflection at the earliest possible stage. In developing and honing the EUISS' foresight skills, the project team are grateful to representatives from the Council of the EU General Secretariat (Integrated Political Crisis Response), European Commission (DGs ECHO and DevCo and the European Political Strategy Centre) and the European External Action Service (EU Military Staff, Strategic Planning Division) for their invaluable input and support. Two workshops were organised by the EUISS on 11 May and 1 June 2017 to engage these stakeholders. Interestingly, once the EUISS team had presented their scenarios and approach at these workshops a wholesome debate between members of the blue team was triggered that raised questions about existing policy mechanisms, lines of responsibility, budgetary resources, chains of command, etc. This is precisely the effect the EUISS wanted to achieve when embarking on this project.

A final word on the ultimate purpose of this report is required. Clearly, this report is primarily aimed at crisis management decision-makers located in the EU system, although think tank analysts, academics and students may also profit from playing as members of the blue team. For example, the scenarios presented may equally be used for classroom-type activities such as mocking, mooting and/or wargaming. Of course, many of the scenarios in this report may give rise to concerns about political sensitivity. A number of the countries and actors mentioned in the scenarios are of direct policy and diplomatic concern for the EU today.

When reading the scenarios, therefore, there may perhaps be a degree of discomfort with some of the scenarios that have been examined and the conclusions that are subsequently drawn. As members of the red team, the authors believe that this emotional reaction to the scenarios is healthy. The ultimate objective of this report and broader project is not just to enhance the imaginative capacities of the EUISS, but to push decision-makers as far away from their comfort zones as possible. As the EU Global Strategy makes plain, the EU needs to equip itself 'to respond more rapidly and flexibly to the unknown lying ahead'.

I. WHAT IF… DAESH ATTACKS A CRUISE LINER IN THE MEDITERRANEAN?

Florence Gaub

It was a cool December night in 2019 when a Daesh commando team attacked and hijacked German cruise liner *AIDAcarmen* in the Mediterranean Sea. The ship was on its way from the port of Haifa in Israel to the Suez Canal, which it was supposed to enter around 23:30. About half an hour before reaching Port Said, two dinghies, each manned with five men, approached the ship. Undetected in the darkness, the terrorists were met by their five accomplices – who had boarded the liner in Palma de Mallorca as regular passengers – on the ship's tail end. From deck three (the lowest deck which is only 7 metres above the water line), two rope ladders were lowered from adjacent cabins, which allowed the dinghy teams to board within only a few minutes.

Shortly before, the squad aboard the cruise liner had disabled the ship's Wi-Fi in order to prevent passengers from sending a distress signal. Armed with assault rifles brought along on the dinghies, the group of 15 seized the ship's bridge, and sealed off those passengers still in the restaurants and bars. The four cabin decks were then also closed off to immobilise the passengers who had already retired to their cabins. The terrorists managed to neutralise the security personnel rather swiftly – the agents were taken by surprise, trained but not experienced in counter-terrorism, lightly armed and outnumbered. Perhaps more importantly, the terrorist team which had been on board from the start had been able to gather vital intelligence concerning the security personnel – size, patrol patterns etc. – over the course of the week that had preceded the attack.

At gunpoint, the captain was forced to reroute the ship from the Egyptian coast towards Libya. The following morning, as the *AIDAcarmen* neared Tobruk, the terrorists released a video on YouTube, announcing the hijacking of the ship with 1,373 passengers and 418 crew aboard – but made no demands. Instead, the group stated that they would randomly execute passengers every other hour in retaliation for the international campaign against the 'Caliphate'. The video made clear that the team had no desire to negotiate, and should a rescue operation be mounted, it would set off a series of bombs strategically placed across the ship to trigger its sinking. The group held off from any executions until midday, when it felt confident that the news had reached most major news outlets: it then chose five men, all of which were Germans, and murdered them. The dumping of their bodies over the ship's rail was equally postponed until the arrival of the world's press for dramatic effect.

By this point, the ship had reached Libyan waters, putting it – at least in theory – under Tripoli's jurisdiction. But the Libyan authorities were neither capable nor united

enough to react effectively: its coast guard approached the ship but kept a safe distance, as did the boats filled with the international press. Given the ship's German registration and mostly German passengers, Berlin had to come up with a plan to solve the crisis as fast as possible. By 18:00 that day, Daesh had executed 40 passengers, and it became clear that any attempt at negotiations or further stalling would only cause more bloodshed. At midnight, the maritime component of the German special operations unit GSG9 stormed the ship; while the bomb threat proved to be a bluff, the terrorists managed to execute several more hostages before being neutralised themselves. In total, 104 people had lost their lives – 89 innocents plus the terrorists.

The consequences

The immediate consequences of the attack were economic in nature, with the tourism industry across the Mediterranean suffering a severe blow – particularly because it was timed immediately before the so-called 'wave season' (the three-month period at the beginning of every year, during which nearly half of all cruises are booked). Before the attack, cruise liners had been an exponentially growing industry, which had generated more than €36.7 billion and 300,000 jobs and attracted over 6 million passengers in 2015 alone. Between 40 and 50 ships serviced the Mediterranean for tourist purposes, with passengers coming mainly from Germany, the UK, Italy, France, Spain and Scandinavia. Cruise companies were forced to review their security measures (until then built on the assumption that terrorists would attempt to smuggle weapons aboard through luggage), a move which had significant financial consequences.

But the more severe impact was of a strategic nature. The terrorists' link to Egypt immediately caused a diplomatic crisis: 10 of the attackers were Egyptians (two from Libya, two from Tunisia and one from Syria), and more importantly had trained with Daesh's outlet *Wilayat Sinai*. Moreover, it was in Egyptian waters that the cruise liner had been attacked, with its coast guard either unable or unwilling to deter the attack. While the German government was reticent to adopt an aggressive approach, its public and media demanded a strong reaction, blaming Egypt's human rights record and repressive policies for the constant simmering of jihadist terrorism in its territory. European cooperation with Egypt was subsequently slammed across European media.

The attack equally underlined the still dissatisfactory state of political affairs in Libya – for which NATO was blamed. This had delayed the rescue of passengers and, more generally, allowed for Daesh to remain a serious threat despite the displacement of the organisation from Iraq and Syria. Anti-Muslim sentiment, already strong, was only strengthened amongst European publics, with demonstrations demanding an end to Arab asylum-seekers and forced readmission. Lastly, the public perception of Western military and civilian operations in the Mediterranean reached an unprecedented low, as the eight NATO and EU ships which had been in relative close proximity to the *AIDAcarmen* had been unable to take action.

Most importantly, maritime security in the Mediterranean was suddenly put under threat. Neither piracy nor terrorism had been an issue in the preceding decades: the last incident had been the hijacking of Italian cruise liner *Achille Lauro* by a Palestinian commando group in 1985, while piracy had not been an issue since the 17th century (although asymmetric warfare during the Second World War was labelled piracy for political reasons). The attack stressed, once again, the necessity not only for an integrated maritime surveillance system for ships crossing the Mediterranean, but also the vulnerability of trade in the sea (15% of global shipping and 29% of European shipping activity takes place in the Mediterranean). That the security of maritime vessels was suddenly called into question once again highlighted the link between European and North African/Middle Eastern security.

Where did it all go wrong?

Three dynamics collided in the attack on the *AIDAcarmen*: the deterioration of the domestic situation in Egypt, the displacement of Daesh from Iraq and Syria, and insufficient security precautions on soft targets such as cruise liners. The first element was a combination of repression in Egypt and inefficient economic and social policies. Although Cairo cracked down on terrorists (suspected and genuine), the failure to deliver on economic reform fuelled further frustration and political discontent. Its counter-insurgency measures in the Sinai only strengthened the bond between local residents and foreign jihadists who arrived on the peninsula after the fall of Raqqa and Mosul. Extreme Port Said football fans – who shared the jihadists' opposition to the government but not their ideology – provided logistical help in preparation for the attack. Lastly, cruise companies did not anticipate an attack of this scale: after the hijacking of the *Achille Lauro*, and the killing of cruise passengers on shore in Tunisia in 2015, companies expected attacks to either happen in country (hence suspending shore leave in unstable countries), or for terrorists to attempt to smuggle weapons on board in their luggage. This underestimation was to ultimately prove costly for the *AIDAcarmen's* passengers, the tourism industry, and the region's dynamics as a whole.

II. WHAT IF… RUSSIA INTERVENES AGAIN IN UKRAINE?

Daniel Fiott

In the summer of 2020, Russian forces entered Dnipropetrovsk International Airport (Ukraine's fourth largest city), blockaded the M34 motorway that links Dnipropetrovsk to Kiev and seized railway lines in the region. At the same time, Russia deployed the *Admiral Grigorovich*, *Ladnyy* and *Smetlivyy* frigates and the *Azov* and *Caesar Kunikov* landing ships in the Sea of Azov, sent air detachments and funneled supplies through the coastal cities of Mariupol and Berdyansk. Paratroopers, tank battalions and mechanised warfare equipment were then deployed to the Kherson, Zaporizhia and Dnipropetrovsk regions via bases in Russia's Southern Military District. Following Russia's seizure of Crimea in 2014, the Russian military had modernised their air and land assault capabilities through regular training – with a view to one day deploying forces in southern and eastern Ukraine. Yet what appeared to be an act of war was in fact an act of humanitarian assistance – or rather, an act of war under the cover of humanitarian assistance.

Indeed, Ukraine was in need of humanitarian assistance due to mass flooding – only Russia went further than that. Once in control of the airport, it impounded all EU aid supplies sent to the region to help cope with the flooding and started its own deliveries of aid and supplies to the region via Crimea and the Sea of Azov. Although international calls on Russia were issued immediately to allow international humanitarian aid into the affected regions, it became clear that Moscow had taken full political and military control of the Kherson, Zaporizhia and Dnipropetrovsk regions. More than 5,000 personnel and 900 pieces of equipment were deployed in the three regions, including *Spetsnaz* brigades and elements of the 4th Air Force such as the Mi-8 transport aircraft and Ka-52 attack helicopters. These were not sufficient grounds for NATO to intervene: after all, this was not an Article 5 situation. Once accused of mainly supplying aid provisions to Russian-friendly populations and rebel groups, Russia expelled all remaining international observers and aid providers from the region. 'What we are seeing in the south of Ukraine is a wilful attempt by Russia to deliver aid selectively and the imposition of martial law', claimed one Western diplomat. Yet ambassadors at the UN Security Council found no clear path forward on how to deal with the humanitarian disaster in Ukraine – especially given the presence of Russian forces on the ground.

The consequences

Russia's decision to deliver aid to the flood-hit regions via Crimea meant that Russia could secure a land corridor through the Dneiper river basin. This effectively drove a strategic wedge into southern Ukraine. Russia immediately deployed *Buk-M3* and *Pan-*

tsir-2 anti-aircraft missile systems to the region in order to dissuade the UN, EU and international aid agencies from flying aid drops. Commercial airliners and military transport aircraft would not risk flying into Ukrainian airspace. NATO could not agree on a military response because Ukraine is a non-NATO member. Nevertheless, Russia's decision to seize the Kherson, Zaporizhia and Dnipropetrovsk regions was not based on a desire to increase its missile strike range *vis-à-vis* NATO allies, for it already had S-300 and S-400 launchers based in Crimea which served to deny access to the Black Sea. Instead, Moscow's aim was to hold territory in order to force political concessions from Kiev. The regions seized by Russia were home to important economic centres for Ukraine. For example, Kherson was home to Ukraine's ship-building industry, Zaporizhia housed numerous port cities and the country's largest steel plants, and Dnipropetrovsk represented more than a quarter of Ukraine's total industrial output, including the production of space rockets and satellites. Seizing industrial assets in this way made it more challenging for Ukraine's government to service its international debt commitments.

Russia's presence in the region soon began to hurt Ukraine's economy. Historically known as Europe's 'breadbasket', Ukraine was home to some of the most fertile soil (known as humus) on the European continent and the sector accounted for approximately 8% of Ukraine's GDP. Russia's aim was principally geared towards holding territory, so usual flood recovery measures such as embankment and drainage repair were neglected. Of immediate concern for the UN and EU was Russia's refusal to allow for disease control in the region. Without an international response, it was possible for diseases such as cholera and leptospirosis to spread – in fact, local media reports claimed that the waste water treatment plant at Zaporizhzhya had already been contaminated. Disease looked to be spreading to livestock in the region, too. This situation was compounded by Russia's decision to indefinitely close the Zaporizhia nuclear power plant near Enerhodar on the grounds that it had been compromised by the 2018 flooding. As a result millions were left without the 6,000 MW of electrical capacity produced by the Zaporizhia plant. In control of electrical power and resources, Russia had achieved full political as well as military control of the region.

Where did it all go wrong?

The groundwork for the events of 2020 was laid in 2018, when Ukraine and its neighbours experienced a particularly warm summer. Already vulnerable in that regard (only 25% of Ukraine's water supplies are formed in country, with the rest emanating from Belarus, Romania and Russia), Ukraine was hit the hardest. While it was traditionally the southwest region which was most vulnerable to water shortages, this time eastern Ukraine equally experienced water scarcity. The problem was aggravated by the fact that eastern regions such as Kharkiv, Donetsk, Luhansk, Zaporizhia and Dnipropetrovsk were now home to more than a million internally displaced persons (IDPs) since the 2014 conflict. But the situation deteriorated further: the combination of warm weather and poor soil quality led to land fissures near the Dnieper hydroelectric dam, compro-

mising the architectural integrity of the dam. Although Ukrainian authorities took initial steps to secure the integrity of the dam over the summer and autumn, efforts were under-resourced and not rapid enough. The warm summer months were then followed by a reversal in temperatures and heavy rains. The increased rainfall and water surge resulted in the Dnieper dam bursting. The burst dam released a sizeable amount of the total 33 km^3 of water it stored into the Dnieper River and the 1,569 MW of the installed capacity of electricity normally produced by the dam abruptly came to an end, leaving up to 1 million homes without electricity supply.

The flood water surge principally affected the cities of Enerhodar (population: 54,500), Nikopol (population: 120,700) and Zaporizhia (population: 767,000). Government efforts were supported by a range of non-governmental organisations (NGOs) and the Ukrainian Red Cross which assisted with logistics and public relations. The Ukrainian military were also called on to help with relief. Yet relief efforts were negatively impacted by the cold turn with areas flooded by the dam breach becoming affected by subsurface frost. Transport and logistical access to the flood and relief area was made difficult given the terrain in the region. Ukrainian emergency response services started to airlift supplies to the region, but efforts to uncover and rescue individuals trapped in the affected flood areas – including EU personnel – proved extremely difficult. There was little to no military and security protection for international aid workers. Although several international organisations were already delivering aid to the regions of Dnipropetrovsk, Donetsk, Kharkiv, Luhansk and Zaporizhzhya because of the conflict, the government in Kiev launched an international appeal for further support to deal with the aftermath of the flood.

This was the entry point for Russia, which offered assistance to the Ukrainian government. Although the experiences of Crimea should have led to more effective early-warning signals and planning, from February 2019 onwards Russian humanitarian support and armed personnel began to move into the region. The flood-hit area was not far from Crimea and the region housed a comparatively higher percentage of Russian speakers than other areas. Although the Ukrainian military did try to repel Russia's advances, hybrid tactics were employed with local militia groups loyal to Moscow supporting Russia's advance into southern Ukraine. Russian forces did not bear any official insignia. Ukrainian forces were loath to attack militias in the region, even if they were supporting the Russians. A combination of Russian disinformation about the dam (with some reports saying that the dam was purposefully destroyed by Ukrainian nationalists to precipitate conflict with Russian-speaking Ukrainian minority groups) and its missile defence systems in Crimea, effectively dissuaded serious Ukrainian retaliation. Although the alliance stepped up air patrols in the region, these same tactics ensured that NATO did not intervene to repel Russia's seizure of the Kherson, Zaporizhia and Dnipropetrovsk regions.

III. WHAT IF... ISRAEL AND HIZBULLAH FIGHT ANOTHER WAR?

Julia Lisiecka

The assassination of Mustafa Mughaniyeh, a top Hizbullah military commander, in the Syrian Golan Heights in early April 2019 through an Israeli airstrike did not seem to be particularly alarming news: Israel had repeatedly breached Syrian airspace during its neighbour's civil war, taking advantage of both the regime's and Hizbullah's war fatigue. This time, however, the incident did not end with the usual round of threatening political statements and exchange of fire on the border: in a televised speech, Hizbullah's leader, Hassan Nasrallah, stated that if Israel did not immediately retreat from disputed Shebaa Farms – a small piece of land which lies between Syria and Lebanon and has been effectively under Israeli control since 1967 – the organisation would use its long-range missiles to strike a chemical plant in Kishon near Haifa. In return, Israel's Chief of Staff, Gabi Eisenkot, announced a new military operation in Lebanon, stating that 'Israel holds the Lebanese government accountable for all actions taken by Hizbullah'.

Soon after, the Israeli air force began striking Hizbullah and Lebanese Army Forces in Beirut, southern Lebanon and Beqaa Valley. Hizbullah retaliated with an intense barrage of rocket fire, which reached as far as Tel Aviv and the Tamara offshore gas rig. Shebaa Farms became the centre of ground clashes, but fighting also occurred to the east and west along the Lebanese and Syrian-Israeli borders. Hizbullah was capable of launching up to 1,000 missiles a day (10 times more than during the last conflict in 2006), leading to the displacement of half of Israel's population in the north. Even bigger population flows were observed in Lebanon and Syria where already poor access to food, medical services and energy supplies were further curtailed due to the destruction of infrastructure. The airports in both Beirut and Tel Aviv were closed to civilian traffic, while energy plants in both Lebanon and Israel sustained critical damage.

In contrast to the previous war, Hizbullah was now able to sustain a multi-front scenario, which extended combat activities and placed immense socioeconomic stress on both conflict parties. Lebanon suffered over 1,000 casualties, many of them civilian. And although fatalities on the Israeli side were largely avoided as a result of its effective anti-missile system, Hizbullah managed to take 10 families hostage from the Kibbutz Menara bordering Lebanon; their fate remained unknown.

While talks at the United Nations stayed inconclusive, the United Nations Interim Force in Lebanon (UNIFIL) and United Nations Disengagement Observer Force (UNDOF) announced a temporary withdrawal from the Israeli-Lebanese and Israeli-Syrian borders. But most of the troops remained trapped in the warzone and were forced to wait

for a ceasefire to be evacuated. Meanwhile, several dozen members of the Iranian Islamic Revolutionary Guard Corps (IRGC) were dispatched to Lebanon travelling through Iraq and Syria, and Israeli Prime Minister Benjamin Netanyahu left for Moscow with the hope of convincing Russian President Vladimir Putin to use his leverage to deter further Iranian and Syrian involvement in the hostilities.

The consequences

As was the case with the previous war of 2006, the conflict plunged Lebanon back into a political and economic crisis. Saudi Arabia, the most generous donor to Lebanon following the 2006 war, announced it would not provide any more financial support to a country it sees as dominated by Iranian-sponsored Hizbullah. As a result, Lebanese officials were forced to call on the European Union to provide funds for humanitarian assistance and reconstruction efforts, estimated to cost over $15 billion and take over 10 years.

Despite facing criticism, initially Hizbullah seemed to regain the trust of the Lebanese Sunni population (eroded by the group's participation in the Syrian civil war) by presenting itself as the legitimate defender of the rights of Palestinians. Yet the emerging humanitarian crisis soon undermined fragile power-sharing agreements between Lebanese political parties, leading to the first major parliamentary standstill since the 2017 elections.

But the problem is not only domestic: the war further destabilised a region which was recovering slowly from the Syrian conflict, with huge numbers of people forced to seek refugee beyond Lebanon. The growing number of internally displaced people (IDPs) which spilled over to other Mediterranean countries became a major concern for international organisations and European governments. Over 900,000 people fled towards Aleppo in Syria, in hope of crossing the Turkish border, while others attempted to cross the sea to Cyprus. The war also mobilised numerous militant groups throughout the region, causing further alarm not only in Israel, but also in Egypt and Saudi Arabia, which demanded that the UN and EU penalise Iran for its alleged financial support to the Houthi militias in Yemen. These tensions undermined Europe's recent *rapprochement* with Iran, as well as the feasibility of further implementing the nuclear deal.

The open conflict between Hizbullah and Israel has also undermined the fragile alliance system in the region. In previous years, Russia had established itself as a key player in the Middle East through a sort of political balancing act: providing strategic support to Iran and Hizbullah while increasing military coordination and economic ties with Israel. The military confrontation put Putin's *realpolitik* into question; taking Hizbullah's side could have led to a regional spillover of the conflict and even drawn in the US.

Aware of this risk, the European Union was forced to rely on Russia's de-escalation mechanism to reach a ceasefire between the two sides. The 16 EU countries involved in

UNFIL and UNDOF missions on the borders (with over 3,600 European soldiers under fire), were cautious about taking any decisive steps which could affect the fate of their citizens.

Where did it all go wrong?

In the context of a changing geopolitical environment, the violent rhetoric and limited exchanges of fire between Hizbullah and Israel (which for over a decade served solely as means of deterrence) suddenly became a conflict trigger. The slippery-slope scenario took the international community, which had overlooked the growing willingness of both sides to get involved in another military confrontation, by surprise. However, for the political leadership on both sides of the border, war was increasingly seen as the only solution to the perceived challenges they faced.

Israel had long observed the growing military capabilities of Hizbullah, which had been showcased during the Syrian conflict. Russian military expertise and the acquisition of new weaponry through an uncontrolled route leading from Iran had only made matters worse. These included medium- and long-range missiles, such as the surface-to-surface Scud D, which has a range of up to 700 kilometres, the surface-to-air S-300, and the surface-to-sea *Yakhont*, which could be used against offshore gas rigs. Political elites in Tel Aviv felt under increased pressure to reduce these capabilities before Hizbullah could be, as feared by Israelis sceptical about the nuclear deal, covered by an Iranian nuclear umbrella.

When the war in Syria slowly began to peter out, Hizbullah started exploring ways in which it could use the new strategic depth gained through its presence in the Golan Heights. The group also hoped to re-connect with its base and recover from the damage to its reputation caused by its engagement in Syria. Hizbullah was also well aware that Lebanese Armed Forces, which had sustained major damage during Israeli air raids, were unable to capitalise on the investments made in the previous years, including by the European Union and its member states, and faced resource shortages following Saudi Arabia's grant freeze in 2016. Through a psychological and propaganda victory, Hizbullah hoped to strengthen its independence, avoid the oversight of civilian authorities, as well as generate a unifying narrative for its ally – the Syrian regime still struggling to regain full control over its territory.

IV. WHAT IF... BOSNIA-HERZEGOVINA DISINTEGRATES?

Zoran Nechev

'Today, we are finally liberating ourselves from this artificial and so-called state of Bosnia-Herzegovina...' announced Milorad Dodik, the former president of Republika Srpska (2010-2018) and now prime minister, to a large crowd of Bosnian Serbs who had gathered in Banja Luka.

Within an hour of Dodik's announcement, hundreds of Bosniak war veterans and their supporters gathered in the heart of Sarajevo, chanting their opposition to 'the birth of a genocidal state' and calling on Europe to prevent Republika Srpska from seceding. In a press conference the same day, the Bosniak member of the Bosnian presidency condemned the move in no uncertain terms: 'Bosniaks will not accept something established on ethnic cleansing and mass killing to become a state. We will fight against it with all the means we have.' Bosnian Croat leaders mainly felt vindicated by events, seeing it as proof that the decision of the Bosnian Croat political parties 'not to take part in the unconstitutional and illegal elections in 2018' was the right one.

The inflammatory rhetoric was quickly followed by violence: the next morning, six bombs simultaneously exploded in Bosnia's four most important cities Banja Luka, Sarajevo, Mostar and Brcko, and a group of men singing Serbian nationalist songs vandalised the Srebrenica genocide memorial centre. During the night, Bosnian Serb police forces and Serb-dominated units of the armed forces entered the disputed city of Brcko, thereby linking the disconnected eastern and western parts of the Republika Srpska and establishing communications with Belgrade. The state of Bosnia-Herzegovina (BiH) was about to cease to exist.

The consequences

Within days, BiH had returned to its 1995 frontline situation, with the three major ethnic groups managing themselves administratively. Whereas Sarajevo tried to reverse Milorad Dodik's move, Bosnian Croats continued their (since 2018) *de facto* self-rule. Online jihadist groups jumped at the occasion to garner Bosniak support and called for violence against Serbs and Croats in Bosnia-Herzegovina.

At the international level, the most rapid response came from Russia and Turkey. The Russian foreign ministry called on all sides to keep the peace, but boasted that 'the West's policy of undermining the rights of Serbs and Croats in post-1995 Bosnia, combined with its open support for those who sympathise with the agenda of Islamic extremists, has officially failed.' At the United Nations Security Council, Russia's ambas-

sador objected to UK-US calls for an emergency session on the crisis, explaining that 'Russia is now working closely with Turkey and other partners in the region on a new initiative for Bosnia. The EU and the West are no longer considered to be honest brokers in Bosnia or the region.'

Meanwhile, Turkish President Erdogan declared that he 'and the Turkish people stand ready to protect their Bosniak Muslim brothers and sisters.' Serbia quickly got involved, too: President Aleksandar Vučić, now in his second term, and Croatia's Prime Minister issued a joint statement calling on all parties to refrain from resorting to violence. More controversial rhetoric came from Croatia's president while out on the campaign trail: 'should the Republika Srpska's secession succeed, 400,000 Croat Catholics cannot be abandoned in a failed state full of Muslims who openly sympathise with ISIS'

The Austrian and Slovenian media were the first to broadcast news about Frontex preventing hundreds of Bosnians from crossing the border with Croatia. Meanwhile, the Bosnian diaspora started to organise protests in all major Western European capitals.

Finally, the EU's EUFOR mission was unable to prevent the crisis from occurring. First, because it did not have a back-up plan once Russia blocked the prolongation of the Chapter VII mandate for EUFOR in the UN Security Council. Second, because it did not establish an adequate military presence in the strategically important Brcko district.

Where did it all go wrong?

The biggest driver of the crisis was that some of the most prominent Bosnian political figures opted to distract the population from the country's difficult socio-economic situation with ethnic tensions and political disagreements. In 2017, almost half of the country's total budget was spent on repaying past loans. Revenues were generated through taxes, new loans and the selling of state assets. At the same time, BiH struggled with a large trade deficit, was unable to attract much-needed foreign direct investment (FDI), and its economy and citizens were dependent on remittances from diaspora.

The covering up for the difficult socio-economic situation with fights over ethnic and constitutional issues was already visible in 2016. During the summer of 2016, Bosnian politicians clashed over ethnic aspects of the census results, and then in September they fought about whether or not to hold a referendum on a holiday in Republika Srpska. In late 2016, there were more disagreements over how to interpret the call by the European Parliament for BiH to undertake constitutional reforms in order to become fully federalised. And throughout 2016, rival politicians fought over who sits and decides in the EU coordination mechanism. 2017 then saw the revival of a lawsuit against the Republic of Serbia for the Yugoslav wars. The EU's active (and passive) role in these and later developments left the Union with little or no influence once the crisis erupted.

Transparent lobbying efforts by Croatia in 2016 yielded results: changes to the electoral law in BiH became a condition for the country to be awarded EU candidate status. But this did not help Bosnian politicians reach a compromise. Instead, it provided them with a topic they could fight over and use to fire up their electoral bases. The EU's conditionality and failure to change the electoral law by the 2018 general elections encouraged Croat political parties to decide to boycott the vote – effectively paralysing the state and entity institutions. In the eyes of non-Croats, the EU was perceived to be favouring one side, something which only served to strengthen anti-EU narratives.

The EU's accession negotiations – its most effective foreign policy instrument – were then suspended. As a result, no progress was made on strengthening the rule of law and fighting corruption. The EU did not do enough work to assess and prevent the radicalisation of the Muslim population in BiH, nor did it collect or spread credible, reliable and up-to-date information on the country's situation. This played into the hands of Russian media outlets and Republika Srpska's president, who since 2016 had started using questionable data about the rise of extremism in BiH to portray Bosnian Muslims as religious extremists.

In addition, the EU did not engage sufficiently in explaining the benefits of the accession process to the public. It also did not insist that the Bosnian government implement and adhere to EU standards in areas that would improve the lives of citizens (road safety, air pollution, public procurement, etc.) Moreover, the pledge made by the President of the European Commission, Jean-Claude Juncker, not to allow any new accessions until at least 2019 further complicated the situation, leaving those politicians who wanted to bring BiH closer to the EU without an actionable platform.

V. WHAT IF… EUROPE IS STRUCK BY RIGHT-WING TERRORISM?

Annelies Pauwels

The death toll of the February 2020 terrorist attacks in the Western European country of Karolia was particularly high: 324 dead and more than double that number injured. Within ten minutes, five car bombs had detonated in three different cities. The explosions hit Parliament, the headquarters of the ruling Conservative Party in the capital Säntjana and two police stations in the south of the country. Meanwhile, leaders of fellow EU member states strongly condemned the attack on innocent civilians and expressed their solidarity with the Karolian people. It quickly transpired however, that, for once, Daesh was *not* behind the attacks as initially suspected: the atrocities had been carried out by Fight-For-Values (F4V), the violent wing of the European Counter-Jihadist Movement (ECJM). The three men – former soldiers of the Karolian army who had also fought in Ukraine as volunteers – who had organised the attacks were quickly apprehended by the authorities.

F4V had been on the radar of the Karolian (and European) intelligence agencies for a while as it had absorbed individuals involved in attacks against refugee camps and mosques across the European continent. While the group advocated aggressive integrationism (requiring proof that immigrants conform to 'European liberal values'), it also used violence to spread fear among Europe's immigrant population and thereby deter migration. At his trial, one of the perpetrators of the terror attacks stated that civilian deaths were, in this context, 'unavoidable collateral damage (…) necessary to replace the national government with a nationalist regime'.

Although F4V had been known to the Karolian Intelligence and Security Agency (KISA), the highly sophisticated nature of the February attacks nevertheless caught the country's intelligence community off guard. As an in-depth KISA report in November 2020 showed, the terrorist group had managed to develop, ever since its formation in 2016, into a highly-organised network with local branches across a number of EU member states. The report also revealed links to a violent branch of the American organisation 'Stop Islamization of America' (SIOA), as well as an Israeli umbrella organisation of violent ultra-Orthodox groups. Moreover, since 2018, some of the highest-ranking F4V members had regularly benefited from financial transfers originating from a number of private bank accounts registered in Russia.

The consequences

The February 2020 attacks marked the beginning of an escalation of terrorist violence across the EU. Karolia, for instance, witnessed an almost 500% increase in terrorist attacks between 2020 and 2025 compared to the previous five years. Most of the violence was attributable to F4V, but smaller networks and lone actors, inspired by the group's ideology, also carried out attacks. The right-wing violence allowed jihadist terrorist networks to intensify their attempts to radicalise Karolia's immigrant and domestic Muslim populations. Indiscriminate right-wing attacks and inadequate law enforcement protection measures gradually led to increased sympathy for jihadist narratives among Muslim communities.

By 2025, Karolia's society was more divided than ever. Surprisingly, F4V enjoyed widespread public support: a public opinion poll showed that 62% of Karolians sympathised with the group's ideology, while 34% defended its violent actions. The increasing frequency of collective right-wing 'hive' terrorism supported the results of this poll: spontaneously-formed crowds, mainly composed of everyday citizens with no criminal background, began to attack Muslim and migrant communities before quickly disbanding after the incident. Due to this development, police authorities found it increasingly difficult to prevent and punish hate crimes.

Government officials were unsure of how to apply their counter-radicalisation programmes – set up ten years ago to fight jihadism – to the wave of right-wing extremism. This was largely due to the fact that Karolia's centre right and far-right had progressively converged over the last three decades, meaning that radical opinions had become mainstream and socially acceptable. As a result, the whole concept of radicalisation, central to the government's preventive counter-terrorism approach, was not fit for purpose.

Where did it all go wrong?

A closer look at F4V's manifesto shows exactly 'where it all went wrong'. The 69-page document that was published online by the group in March 2025 clearly laid out the network's ideology, reasons for action and its political objectives. A central theme throughout the document was anger towards the ruling political class: 'The people of Karolia have been abandoned by the political elite, who defend the gradual destruction of Western society by Islam under the banner of a "multicultural society", rather than focusing on bringing back jobs and factories to Karolia. (...) The only political party which promotes the voice of the people – the Karolian Counter-Jihadist Movement (KCJM) – has been excluded, since its inception, by the political establishment through the formation of multiparty coalition governments. As a result, our organisation must resort to violence in order to preserve Karolia's values.'

The dire economic situation in Karolia had provided fertile ground for this sense of exclusion: in 2017, Karolia already had an unemployment rate of 10.2%, but the 2018

financial crisis had increased this figure to 17% (42% among the youth). The 2019 labour reforms had slightly increased the employment rate, but many of those who lost their jobs after Karolia's main labour-intensive industries relocated to cheaper locations found themselves without alternative employment opportunities.

The frustration of native Karolians with their country's economic situation intensified as a result of the government's poor handling of the large refugee and migrant flows, many of which hoped to reunite in Karolia with previously-migrated family and friends.The expensive (but short-sighted) integration framework for newcomers added to the high levels of public debt but yielded limited results: for instance, the centralised housing system for recognised refugees concentrated newly-arrived migrants in poorer, deprived areas with limited employment opportunities, which, in turn, increased their dependence on the country's welfare system, as well as their likelihood of resorting to crime.

The November 2025 report of Karolia's Parliamentary Intelligence Oversight Committee also shed light on some key causes of the crisis: the report reveals several errors by KISA with regard to the spread of right-wing terrorism. The agency had ignored the increase in right-wing terrorist cells since at least 2015, as they had focused all their attention on the jihadist threat. This pattern could be seen in other EU member states, too: in its Terrorism Situation and Trend Reports, for instance, Europol had repeatedly warned of the threat posed by Europe's right-wing extremists and highlighted the insufficient response of national law enforcement agencies (for instance, low arrest and conviction rates).

The Committee's report also revealed that KISA had not sufficiently monitored returning right-wing foreign fighters – either from the conflict in Ukraine or from Syria and Iraq, where they had fought Daesh alongside Christian and Kurdish militias – and that the returnees had a significant impact on the formation of F4V. Despite KISA's focus on jihadist networks, the report highlighted several flaws here as well. For example, counter-radicalisation efforts had failed to focus on jihadists targeting Karolia's refugee camps: in the same way that a number of Syrians were recruited by Daesh in 2015, cells linked to Boko Haram had targeted Nigerian asylum-seekers who had left their country when violence escalated there in 2018.

KISA had also overlooked Russia's support for Karolia's far-right movements. Russia had served as an inspiration for Europe's far-right movements due to, *inter alia*, its strong-arm approach towards jihadist terrorism, its prioritisation of national independence over multilateral cooperation, and its opposition to secularisation. Already in 2015, Moscow had supported Karolia's far-right both financially (by funding the KCJM's electoral campaigns, for example) and militarily (by setting up training camps in Russia and sponsoring FSB-linked Russian martial arts clubs across the EU). Moreover, Russia, but also other foreign powers, had exacerbated Karolia's social divides by inciting anti-government manifestations and sponsoring a number of alternative media outlets. These unchecked channels continuously spread fake news items about government (in)action and the country's immigrant population, for instance, thus providing propaganda for radical groups.

VI. WHAT IF... THE US MISREADS TURKEY?

Roderick Parkes

In the course of a single day, 24 July 2020, Turkey sharply increased its military presence in three spots – the eastern Aegean, the eastern Mediterranean and – most worryingly for US observers – at key transit points along the Turkish border just north of Mosul. Turkish diplomats said the massive build-up of personnel and vehicles was about migration control: Turkey was plugging a new surge of refugees and terrorist fighters who were being squeezed in all directions out of Syria and up towards Europe. But US intelligence and satellite surveillance found no evidence of these flows.

The US diagnosed instead an act of hybrid warfare: Turkey was using migration control as a cover for military ends. After all, in the recent Geneva talks on the future of the Middle East, President Erdogan had failed to articulate reasons for his country's growing military engagement in the region, complaining only about its historic loss of territories. US analysts predicted Turkey's next step, too: Ankara would renege on its hated 2016 migration deal with European governments. It would push the two million Syrians still sheltering in Turkey up into the Western Balkans, exploiting the chaos.

The US response was swift and well-practised. (The Pence Administration had in fact been preparing for just such scenarios which might split NATO and force the EU to activate independent defence capabilities created during Trump's tenure.) President Pence invoked a NATO summit under Article 4, and called upon Turkey (which had previously invoked the article itself) to explain itself to its fellow allies. A shame-faced President Erdogan was unable to explain his country's actions, limiting himself to new outbursts of anti-Western rhetoric at home and introducing further travel restrictions on Turkish citizens heading for the West.

But shortly after Turkey withdrew its vessels and personnel, the rumours started. Information began to circulate that Ankara had indeed been engaged in migration control.

True, there were no major refugee flows across the Turkish-Iraqi border. But this was only because Turkey had pre-empted them. Ankara, far from resenting the EU deal, had quietly made it central to Turkey's whole model of migration control. Back in 2016, when Turkey had agreed to seal off its border to the EU, it found that it considerably reduced the pull across its southern border to Iraq. By now trying to seal off that border to Iraq, Turkey was hoping to alleviate the pressures further downstream on the Iraq-Syrian border.

In the waters around Lebanon, meanwhile, Turkey is now said to have been shuttling border technology and technical specialists in from Northern Cyprus. This constituted

Ankara's (necessarily low-key) response to the shaky border controls which it believed exacerbated the Levant's geopolitical tensions and risked disrupting the flow of goods.

As for Turkey's blockade of the eastern Aegean, this – it is now being said – was motivated by a simple but shameful goal: to prevent the outflow of Turkish citizens to Europe. Thanks to travel restrictions, Turks could no longer flee their country's repressive regime by air, and they were increasingly taking to the sea.

The consequences

The irony is that the prime effect of the US response in 2020 was thus to unleash an even bigger flow of migrants to Europe: two years later, in 2022, European governments experienced a huge influx of migrants up out of the Horn of Africa. When European authorities finally came to analyse the causes of this flow of people from a region of 180 million, they had to concede that 2020 was a key turning point.

After 2020, Turkey increased its support for Islamist political forces in the Horn. This fuelled religious radicalisation, including of Christians. Intricate ethnic and tribal systems broke down, and large numbers of Muslims fled. They moved up easily through the Levant, where border controls had deteriorated, and up across Turkey's porous southern border. They even moved with ease across the Aegean and up through the Western Balkans, which had become more fragmented since Turkey had abandoned its support for their western orientation and put its faith instead in Chinese investments there.

For years Ankara had been encouraging Turkish Airlines to expand its presence in spots such as the Horn. This diversification of markets had initially come in handy in 2020 as Turkey's economic links with the West slackened, and the airline came to depend on African passengers to make up for the shrinking footfall of Turks. Istanbul airport became *the* hub for well-heeled East Africans moving into Europe. But these businesspeople brought with them illicit smuggling networks, which were activated when the Horn descended into violence.

Where did it all go wrong?

Much of the fault for the misreading of the situation lay with the Pence Administration's reliance on scenario-building. The US State Department, decimated by an outflow of seasoned diplomats, came to rely heavily on these abstract exercises to guide policy. This seemed like a pro-active response to a world which was growing both more uncertain and more hostile. In reality, it became part of the problem: instead of engaging in the world, the US withdrew and speculated about it. And, as US analysts tested their imagination, they ended up reinforcing their prejudices.

In the case of Turkey, the mistrust was mutual. In 2016, for instance, some in Ankara had criticised the US for 'practising hybrid warfare': NATO had just established a naval mission in the eastern Aegean to stem the flow of Syrians into Europe. Critics in Ankara argued that this had pushed Syrian migrants back into Turkey, fuelling the sense of revanchism against the US and Western powers supposedly intent on dismembering Turkey. The government was more sanguine, simply taking it as a precedent to increase the role of the military in Turkey's own border management.

Another telling example came in 2018, when Ankara replaced the Turkish officials involved in the Budapest Process, the migration dialogue Turkey chairs. Ankara's motive was positive: it hoped to use the migration dialogue as a broader Track 2 channel to governments in Europe and the West, and therefore put its most trusted interlocutors in place. But Western countries perceived this as yet another purge of the civil service, and downgraded the dialogue.

In truth, Turkey's interests in its neighbourhood had been straightforward and unchanging for decades – to maintain good relations there. But Turkey had a big mouth, and all too often became trapped by its own words.

Erdogan had used bombastic rhetoric in the 2000s. He wanted to rekindle relations with nearby Ottoman territories, export political Islam to places like the Horn and diversify Turkey's range of international partners to include historic trade partners like China. Then, when the Turkish economy began to shrink, his neo-Ottomanism gave way to neo-Kemalism – an aggressive narrative about exploiting the weakness of the international order. His new theme was revanchism and a desire to avenge Turkey's first president, who signed away contiguous territories. These were empty words designed to fill a strategic vacuum, but they entrapped Turkey.

Tellingly, scenario-planners in the State Department had even predicted 24 July as the exact date for Turkey's monkey business: this was the day of the signing of the 1923 Lausanne Treaty, in which Ataturk gave away Turkish territories. Based on a reading of Erdogan's rhetoric, American analysts predicted that Turkey would exploit this highly symbolic date. And yet, for Turkey's border authorities, 24 July was of significance only because it is the day each year when, statistically, there were the most irregular border crossings as migrants avail of good sailing conditions.

VII. WHAT IF... DAESH SEIZES AN AFRICAN COUNTRY?

Julia Lisiecka and Aleksandra Tor

In November 2020, Daesh controlled 75% of Somalia's territory (excluding Somaliland). It had been more than two years since the jihadist group first seized a city in the country, the sparsely inhabited port city of Qandala in the northeastern autonomous Puntland region. At the time, this was only interpreted as heralding the arrival of Daesh on the continent, but as it turned out, it was the first step in its resurgence. Abdulqadir Mumin, Daesh's self-proclaimed leader in East Africa (and probable successor to al-Bagdadi following the latter's death in late 2017) managed to turn his small group of 150 men into a 10,000-strong, robust and flexible organisation. As a defector from al-Shabab himself, Mumin succeeded in developing Daesh in Somalia into a more international organisation than al-Shabab ever was, accepting foreign fighters and attracting recruits from all over East Africa, as well as from across different sectors of Somali society. Crucially, Daesh Somalia managed to turn itself into the first port of call for fighters fleeing Mosul and Raqqa. Once it was strong enough, Daesh took control of central neighbourhoods in Mogadishu in less than a month in mid-2017, leading to the closure of the international airport and the evacuation of EU and UN staff.

The organisation faced little military resistance: the African Union Mission in Somalia (AMISOM), was forced to withdraw the majority of its troops provided by Uganda, Burundi and Kenya shortly before due to severe budget cuts, and its small remaining mission had not been able to react adequately to the Daesh offensive in the capital.

Worse still, Daesh had not just succeeded, again, in seizing territory, it had equally succeeded in recovering from the severe financial blows it suffered when it lost its Middle Eastern oil income: it moved swiftly into piracy and went on to control 85% of the Somali coastline. Capitalising on the resurgence of piracy which occurred in early 2017 (with the hijack of an oil tanker in March and an Indian commercial vessel shortly thereafter), the group started generating profits from hijackings. The first Daesh-led piracy attack, only months after the fall of Mosul, targeted the French merchant tanker *Esmeralda*, and was successful despite its rather low-key method (two speedboats and small arms).

The group was aided by the fact that maritime security precautions had been relaxed: as only one vessel had been attacked since 2012, NATO's Operation *Ocean Shield* had been terminated just months earlier and EUNAVFOR *Atalanta* had experienced budget cuts. By the end of 2017, over 100 attacks were recorded, out of which 30 were confirmed as piracy attacks – the highest number since 2010. Since the average ransom paid for one hijacked ship was estimated to be approximately $2.7 million, the activity accounted for a substantial part of Daesh's budget. The branching out into piracy was only one of several tactics the organisation adopted to avoid international measures targeting

its financing practices: it became equally active in port taxation, extortion, kidnapping for ransom, smuggling refugees, the sale of uranium, looting and abusing humanitarian aid. Reports suggested that the group managed to generate $200 million in 2017, twice as much as its former rival in the region, al-Shabab. The presence of Daesh on the Somali coast, located close to the strategically vulnerable point of passage – the Bab al-Mandeb choke point – gravely affected trade between Asia and Europe, which decreased from $700 billion to $500 billion in just two years.

The consequences

Daesh's presence in the Horn of Africa had several strategic implications. First, it had severe economic consequences for Europe, as well as elsewhere: the direct cost of Daesh's hijackings reached some $6 billion by the end of 2018. Also trade conducted through the Bab al-Mandeb choke point became more costly because of a 30% increase in insurance premiums. The detour around the Cape of Good Hope, considered a safer route, also increased costs as it extended journeys by up to 3,000 nautical miles, something which resulted in a 30% increase in the costs of transporting oil from the Persian Gulf to Europe. Daesh's presence reversed the trend of oil trade increasing through the Bab al-Mandeb choke point (from 2.7 million barrels daily in 2010 to 4.7 million in 2014), with below 2 million barrels per day eventually passing through. And it was not just Europe which was hit by the choking of one of the world's most important trade routes: Egypt, Libya and Algeria, already facing severe crises at home, suffered financially as a result of a drop in exports.

But the problem was not just economic; although Daesh had so far not executed any crews, its past behaviour in Iraq and Syria suggested that it would do so at some point. In addition, Daesh continued to attract European volunteers – although to a lesser extent than during its Middle Eastern phase. Mumin's own British origins helped brand Daesh's Somalia branch as a truly international outfit: one-third of those who joined its ranks were Muslims of African origin (particularly from Somalia, Nigeria and Senegal), one-third were converts, while the remainder came from South-East Asia or the Arab world. At this point, around 1,000 Europeans had joined Daesh in the Horn of Africa. The foiling of a terrorist attack in Sweden, with operational links to Daesh's Somali presence, raised the spectre of terrorist attacks again occurring across the European continent. Daesh was also able to use its Somali headquarters to extend its network into Yemen, where it managed to stage attacks against Yemeni government forces, as well as its Yemeni rival, al-Qaeda in the Arabian Peninsula (AQAP).

Where did it all go wrong?

The arrival of Daesh in Somalia was, of course, directly linked to the country's own decade-long political turmoil. While the future seemed promising only six years ago, botched elections and the slow pace of political reform throughout 2016 and 2017 altered facts on the ground. In this climate of despair and defeat, Daesh's rhetoric of revolutionary change, coupled with salaries of $500 (higher than those of Daesh fighters in Syria and Iraq, of al-Shabab members or indeed AMISOM soldiers), managed to attract young men, as well as former fishermen who had previously been at the heart of Somali piracy activity. Daesh was, in that sense, more successful than al-Shabab as it appealed not only to different sections of Somali society, but also accepted foreign fighters. Daesh managed to chase out most of the al-Qaeda-linked groups in the region and substantially weaken al-Shabab, which witnessed mass defections. Mumin's faction attracted recruits with a clear and simple ideology, as well as a level of organisation which contrasted sharply with al-Shabab's fragmented structure and theological zeal.

Daesh's re-emergence in Somalia was aided by the international focus on events in Syria and Iraq, as well as by the insufficient attention paid to identifying and tackling the organisation's alternative sources of income. This served as one of the major factors which enabled the intensification of recruitment in Somalia. In Europe, East African communities were not the focus of anti-radicalisation programmes, which primarily targeted immigrants from the Middle East and North Africa. This approach left the significant numbers of Somali diaspora (estimated to number 300,000 people living in the EU, Norway and Switzerland) extremely vulnerable to Daesh's propaganda. Eventually, many would bolster Daesh's ranks in Africa.

VIII. WHAT IF... A COUP IS LAUNCHED IN CAMEROON?

Aleksandra Tor and Alice Vervaeke

Nobody saw the *coup d'état* in Cameroon coming: the country was relatively stable and had no history of military involvement in politics – save for a failed attempt in 1984 when the presidential palace guards had tried to overthrow President Paul Biya. Since then, Biya had won five consequent presidential elections (thanks to his removal of term limits in 2008). However, after the elections in 2018 when the then 85-year-old Biya was chosen for yet another 7-year term with 86.7% of the vote, the country experienced an unprecedented wave of protests, echoing similar demonstrations seen in Gambia and Benin in 2016.

These protests were not just a reaction to the elections, but the result of accumulated discontent. Hitherto leaderless youth groups, which were adversely affected by unemployment more than any other part of society, were now steered by a former opposition activist, Corantin Talla – known as 'General Schwarzkopf'. He had returned from 25 years in exile, and, although he was banned from any political activity, succeeded in mobilising the country's youth (particularly students). The unrest gained traction in Cameroon's English-speaking community, which had faced continued discrimination and had been particularly frustrated since 2017 when an internet ban in the Anglophone parts of the country was introduced.

While security forces managed to keep the protests in check, Biya's ailing health meant he spent more time in Geneva receiving treatment than in the presidential palace. His long absences fuelled internal rivalries within the ruling party and among those close to the circles of power. Critical measures to confront the budgetary and financial crisis were not taken and the International Monetary Fund (IMF) decided to suspend its aid programme. In the North, Boko Haram continued to conduct asymmetric attacks, and the population was angered about the government's neglect of the region.

With the situation continuing to simmer, a group of young colonels led by Jean Mark Nbeke, and supported by generals such as Phillipe Mpay, declared their opposition to Biya and forcefully removed him from the presidential palace in August 2019.

The consequences

Based on the African Union's (AU) policy against unconstitutional changes of government and its Agenda 2063, the coup was condemned by the AU Commission Chairperson Moussa Faki, who led several high-level missions to Yaoundé to negotiate a return of constitutional order. However, the AU Chairman, the President of Niger Mahmadou

Issoufou, together with the Chadian leader Idriss Debry (who was known for his hostility towards Biya), were reluctant to act, seeing the coup as an opportunity to weaken Cameroon. The Economic Community of Central African States (ECCAS) and the Economic Community of West African States (ECOWAS) also failed to react in a decisive manner.

Although the AU condemned the coup, it encountered severe difficulties in its attempts to restore constitutional order in Cameroon. The AU had already suffered from a lack of financial and logistical resources in the past, and had not diversified its sources of external funding. The principle of subsidiarity between the AU and Africa's regional organisations had not clearly been defined and prevented decisive action in such circumstances. For instance, in Libya in 2011 and the Mali crisis in 2012, the AU's response was inconsistent and even contradicted sub-regional initiatives. ECOWAS quickly condemned the Malian coup, but further actions were blocked by the member states. The lack of regional unity created a dangerous precedent for the whole continent, affecting not only democratic stability but also economic cooperation within the regional organisations.

The fact that the coup was not punished encouraged other armed forces to act against unpopular leaders: a new wave of coup attempts in West Africa, such as in Gambia, was inspired by the Cameroonian example. This, in turn, led to African leaders taking countermeasures, securing the loyalty of the armed forces either through punitive or corrupt means. Fearing foreign influence in their armed forces, African leaders curtailed military assistance of any kind, and scrapped professionalisation initiatives (such as those offered by the EU).

Regional cooperation also received a severe blow when the MNJTF (Multinational Joint Task Force) – created by Nigeria, Chad, Cameroon and Niger to fight Boko Haram – was disbanded. The lack of cooperation between the armies of neighbouring countries led to a situation in which the remaining Boko Haram cells could regroup and regain strength. The fact that Cameroon's army was more focused on maintaining control in Yaoundé and elsewhere in the country weakened their resolve to act in the northeast. Following a decisive military campaign in Nigeria, Boko Haram began to look for new safe havens abroad. The group was able to gain ground in Cameroon, where it found a disgruntled population fed up with being marginalised and opposed to the now centralised power structures. Chad also suffered as a result of the situation: although Déby also heavily relied on his army to maintain control and he himself had postponed legislative elections several times, the end of the MNJTF led to a new wave of attacks in Chad and dented his popularity.

Where did it all go wrong?

Two main developments in Cameroon led to the coup: one was internal and related to the armed forces, while the other occurred at a national level.

The military, leading the fight against Boko Haram, had seen its popularity increase, achieving approval ratings of 68% according to data from the 2018 Afrobarometer. Its success was partially due to increased professionalisation: it had received training and equipment from France and other EU countries as part of efforts to improve counter-terrorism measures. In 2015, the Cameroonian army was ranked the 17th most powerful army on the continent; in 2018, it had already climbed to 10th place. This was also the result of tightened cooperation with Beijing: since 2017, China accounted for more than 40% of total arms deliveries to Cameroon, and did not attach any political conditions to its assistance. As the armed forces' popularity rose and his own declined, Biya took steps to ensure the military's loyalty, meddling with new appointments and inflating the number of generals to 35. This frustrated a new generation of middle-ranking officers, as they resented the violation of the meritocratic principles which underpin the military. Due to the increased number of generals, the wages of lower-ranking military officers declined. Their engagement in dangerous anti-Boko Haram initiatives also resulted in these soldiers being overworked. All of these factors negatively impacted the army's morale and reduced its loyalty towards the government.

Furthermore, the weakness of the AU and the failure of regional organisations to react collectively to military interventions in politics had become a constant feature of African politics. West Africa was also the region which saw the most coups (both successful and failed), so the contagion effect could have been predicted. But more importantly, it was the domestic political context which provided the military with sufficient reasons to intervene in politics. The recurrent extension of Biya's presidential terms, the dire economic situation, and the lack of political participation all provided fertile ground for unrest to spread. The state failed to provide services and employment opportunities, which only reinforced the dissatisfaction of youth movements. Non-inclusive politics and a lack of economic growth eroded the legitimacy of Cameroon's leaders, and gradually created the conditions for a coup.

IX. WHAT IF... NORTH KOREA INVADES SOUTH KOREA IN CYBERSPACE?

Patryk Pawlak

South Korea's presidential elections had been scheduled for 17 September 2019, shortly after the three-day long national holiday *Chuseok* when Koreans traditionally visit their ancestral hometowns. Five days earlier, an international group of hackers launched a series of Distributed Denial-of-Service (DDoS) attacks on Korean energy grids and transportation infrastructure, leaving millions of people stranded at train stations and airports. A separate attack performed using an advanced version of the *Mirai* botnet downed several governmental websites, preventing people from receiving updates about the crisis. The access to services was only gradually restored after North Korea suffered a complete internet outage similar to the one that occurred in December 2014 after the US retaliated for the Sony hack. In the meantime, however, the failure of news websites allowed fake news to be spread through a messenger app KakaoTalk. The most shared message suggested that the outages were caused by faulty hardware and software had been purchased by the government without proper public procurement procedures.

As a result, accusations of corruption quickly translated into a significant drop in support for the leading candidate in the polls, Han Hyun-joo, the former minister of science, ICT and future planning and the first female CEO of South Korea's biggest internet company. Memories of the impeachment of President Park Geun-hye were still fresh, and South Korea's public reacted angrily to the accusation; approval rates for Ms Han were down to18.3% within days.

When the election results came in on the evening of 17 September, it appeared she had managed to garner a shocking 82.2% of the votes. Allegations of vote rigging spread like wildfire over social media, with many accusing Ms Han of having tampered with the voting machines. Violent mass protests broke out across the country, plunging South Korea into a serious political and economic crisis which paralysed the whole country.

The consequences

In light of doubts about the validity of the election, the National Election Commission launched an investigation into the possible violation of electoral law. After several weeks of investigating, the Commission – using its newly awarded powers – concluded that the election results had indeed been tampered with. They found evidence that during the online transmission from local election committees, all votes cast for Ms Han's

opponents were changed to her advantage. Thanks to support by forensic teams from France, Germany, the UK, and the US, the Commission also established that the interference was *external* and that Ms Han had not been involved: the team of experts subsequently traced the attacks back to North Korean hackers from the Kim Il Sung Military Academy. The time stamp of the malware code suggested that the intrusion took place on 12 September 2019. The recurring reference to *Ssireum* – the most popular Korean sport played during *Chuseok* – was used as a metaphor for a struggle between North and South Korea. It later became clear that the DDoS attacks in September had been a decoy to distract the security services, while the social media campaign was aimed at creating political instability. However, the draft resolution of sanctions against North Korea proposed by South Korea – a non-permanent member of the UN Security Council – was blocked by China and Russia who argued that the evidence on attribution of the attacks submitted by Seoul was 'unsatisfactory' and 'inconclusive'.

The investigation into the attacks against South Korea attracted significant international attention, especially ahead of the Tokyo Olympics in 2020. The investigation by the UN High Representative for Stability in Cyberspace – a new position established in 2020 – concluded that because nearly all of North Korea's internet traffic was routed through China, the latter had possessed the means to prevent or at least minimise the consequences of the attacks. Drawing lessons from the South Korean experience, and in light of limited progress towards the adoption of global cyber norms, a revamped version of 'cyber toolkit' was adopted by the European Union during the French Presidency in 2022. By 2025, the European Union adopted several bilateral cyber stability agreements with third countries such as Brazil, Belarus, China, Russia, South Africa, the UK and the US.

The evidence that the cyber mercenaries affiliated with the North Korean regime had operated out of India, Kenya and Nigeria further demonstrated the need to clarify state responsibilities in the cyber domain. Such a discussion, however, had been stalled since 2018 when international attention shifted from debate about how existing international laws apply in cyberspace towards the cumbersome process of international treaty negotiation. The main division lines were drawn regarding the role of non-state actors in the process and the definition of a cyber attack. The cyber domain remained a contested space.

Where did it all go wrong?

Ironically, it was a series of hacks during the 2018 Winter Olympics in the South Korean province of PyeongChang which had prepared the ground for the events of 2019. Then, cyber-operation #OpGam – a reference to the 'gam' trigram in the South Korean flag signifying the moon, winter, wisdom, but also north – conducted by a group of North Korean hackers resulted in the hijacking of websites and social media accounts of the Korean Ministry of Interior, Ministry of Foreign Affairs, and several tourism offices.

They were then used to disseminate false travel advisories, resulting in numerous cancellations. Critical infrastructure was also affected: a ransomware attack occurred on the Seoul subway system similar to the one on the San Francisco Municipal Transportation Agency in November 2016, and the official Hello PyeongChang mobile app was breached by hackers associated to the North Korea government, which affected over 37 million devices worldwide.

Such a broad scope of malicious cyber operations was partly facilitated by the large amount of data that was available online in the framework of Government 3.0 programme launched in 2014. In an effort to promote a 'creative economy' and public administration transparency, all levels of government and public corporations had provided large amounts of data in 11 sectors, including public finance, national health, and law enforcement via the government-run Public Data Portal. In total, the 'PyeongChang disaster' cost the South Korean economy the equivalent of 2% of its GDP.

When Ms Han was appointed minister following the cyber-attacks, she launched a series of reforms designed to turn the dream of a 'Digital Korea' into reality and strengthen the country's cyber resilience. By 2019, South Korea became the first country in the world to provide access to internet to all its citizens. For the first time in history, presidential elections were fully conducted online – an opportunity to showcase Korean leadership in e-government solutions and confidence in the digital domain. However, these efforts were not matched by an adequate resilience-building strategy.

Several internal and external factors contributed to Ms Han's failure. The rollout of the connectivity programmes was not accompanied by targeted awareness-raising campaigns about digital risks stemming from increased connectivity. Furthermore, it later became apparent that the supply chain of the South Korean company that won the tender for delivering e-election solutions was heavily dependent on systems produced by Chinese suppliers. Finally, convinced of its digital superiority, the South Korean government ignored the lessons from cyber history and the fact that in the cyber domain great damage can be caused by adversaries with limited resources.

The absence of a decisive international response following the PyeongChang attacks only reinforced the feeling that malicious activities could be conducted in cyberspace with impunity. For instance, proposals included in the 2017 report by the UN Group of Governmental Experts aimed at strengthening cooperation between states were not implemented, undermining the international response mechanisms. The debate about the diplomatic response to cyber-attacks that intensified following the strengthening of US sanctions against North Korea in 2019 only further alienated the two respective camps grouped around Russia and China, and the US.

X. WHAT IF... JAPAN GOES NUCLEAR?

Eva Pejsova

In the end, Tokyo followed the suggestion made by President Trump on his campaign trail and decided to develop its own nuclear capability in 2020. Several developments had led to this drastic break with Japan's long-standing pacifist policy: North Korea's added intercontinental ballistic missile capability to its already frightening nuclear programme, proudly announced by the country's dictator Kim Jong-un during his 2017 New Year's address and tested shortly thereafter. Although missile tests had repeatedly come close to reaching Japanese territory in the past, this development, coupled with North Korea's historical and ideological resentments towards Japan, led Tokyo to believe it was one of the main targets of any possible attack.

China's continued military growth and modernisation had long been a major source of anxiety for Tokyo's security analysts and decision-makers. For them, Beijing's rising strategic ambitions in the region, especially visible in its increasing assertiveness in the East and South China Seas, constituted a direct threat to Japan's national interests and sovereignty. Finally, Russia's deployment of anti-ship missile systems on two of the four disputed Kuril Islands in late November 2016 was the final straw for Japanese policymakers, who already felt that Japan was disadvantaged as the only major player in the region without its own nuclear deterrent (the US, China, Russia and India are all nuclear states).

The arrival of a new, more isolationist administration in Washington, Japan's key security ally, only compounded this threat perception. While the Trump administration showed itself to be less committed to Japanese security than previous US governments, it was also more confrontational towards China and North Korea – essentially leaving Japan in charge of both its own and US interests in the region. With its new nuclear capacity, Japan hoped to recalibrate regional relations, deter North Korea, create bipolar stability (an idea underpinned by the nuclear peace theory) and enhance its bargaining power. When combined with the long list of external dangers, these perceived benefits were sufficient for Japan to bid farewell to its traditional peaceful profile in view of preserving the regional *status quo*.

The consequences

As it turned out, the nuclear peace theory had its limits in North-East Asia. North Korea, still officially and *de facto* at war with the US and its allies since the end of the Korean War in 1953, considered the acquisition of a nuclear potential by Japan as an open threat and provocation. Given the hardline ideological stance of the regime and the strong conditioning of its population, the threat of mutually assured destruction or

enormous loss of civilian lives did not have the deterrent effect that Tokyo had hoped for. China, the long-standing historical and ideological ally of the Pyongyang regime and a nuclear power itself, double-downed on its commitment to the Kim regime as it saw Tokyo's nuclear step as an inherent threat to its ally, as well as its own national security.

This perception resonated across the region, concerned about the possible resurgence of Japan's past imperialist tendencies. North and South Korea – more than at odds politically – remained united in their rejection of what both governments saw as a precursor of Japanese expansionism. China became the most vociferous critic of Japan's re-militarisation, boosted its own nuclear programme and marshalled the support of other nuclear weapon states – including Russia and Pakistan. Tokyo's move therefore triggered further repercussions across the Indo-Pacific region, with both India and the US stepping up the game in defence of their own national interests. The risk of miscalculation and accidental warfare reached new heights, keeping the entire Indo-Pacific region in a permanent state of tension.

Where did it all go wrong?

Several developments had prepared the ground for Tokyo's decision in the long term. The Japanese domestic political environment had become more ideologically tainted in preceding years. After almost two decades of economic slowdown, right-wing nationalistic sentiments were on the rise. A number of nationalist groups (*uyoku dantai*), nostalgic about Japan's past military strength and imperial glory and promoting its exceptionalism, had been pushing for the country to develop greater security independence in light of mounting regional tensions. While those groups first accounted for a small minority of the total population, patriotic views had become mainstream under the administration of Prime Minister Abe.

Conference Japan (*Nippon Kaigi*), a highly influential nationalist lobby group advocating the revision of Article 9 of the Japanese constitution (which outlaws war as a means to settle international disputes) and promoting historical revisionism, gained substantial support in both chambers of the National Diet, and its members constituted the majority of the ministerial cabinet already by 2016. Prime Minister Abe's determination to 'break away from the post-war (pacifist) regime' started with a new security strategy and the promotion of legislative amendments allowing Japan to play a greater security role in the region and beyond. The legal extension of his premiership until 2021 allowed him to further work towards constitutional reform.

And while Japanese society remained historically attached to pacifism and concerned over nuclear safety (particularly in the shadow of the 2011 Fukushima Daiichi nuclear power plant disaster), against the backdrop of a looming North Korean nuclear threat, changing regional balance of power and persistent economic slowdown, voices in favour of the constitutional revision became louder. The young generation, brought up

detached from post-war memories, started to perceive Chinese and Korean criticism of Japan as belligerent and unfair, and threw their weight behind the idea of a strong, strategically autonomous Japan.

In the past, Japan had already considered the acquisition of small tactical nuclear weapons for defensive purposes on several occasions. In 1970, when Japan signed up to the Non-Proliferation Treaty (NPT) and in 1998, when North Korea tested its first nuclear missile (Taepodong-1), the debate resurfaced, but on both occasions the US nuclear umbrella was considered sufficient. However, this element had now been removed from the equation. Decades of investment in peaceful nuclear scientific research had made Japan a champion in the domain. From a resource point of view, Japan possessed sufficient amounts of reactor-ready plutonium, as well as enriched uranium, to produce a significant number of nuclear missiles. It always had all the necessary technology, skills and facilities to produce a nuclear weapon within months; eventually, it did precisely that.

XI. WHAT IF... CONFLICT ERUPTS BETWEEN INDIA AND PAKISTAN?

John-Joseph Wilkins

An unexpected explosion in the Thar Desert in Rajasthan propelled India and Pakistan into the worst crisis since the 1999 Kargil war. The strike, which hit an Indian Army Armoured Corps regiment while it was out on manoeuvre close to the Pakistani border, appeared to have been carried out – without government approval – by a rogue and radicalised commander in the Pakistani air force. Unlike India, Pakistan had refused to commit itself to a 'no-first-use' policy, something which initially helped convince alarmed policymakers in New Delhi that Islamabad had sanctioned a form of tactical nuclear attack. The Indian government immediately responded with artillery targeting Pakistani outposts in Kashmir, while India's Western and South Western Air Commands scrambled their planes. A fleet (including India's only aircraft carrier, the INS *Vikramaditya*) was dispatched to patrol India's western coast in a show of strength.

Meanwhile, Pakistan's response was swift and unprecedented: the Pakistani Prime Minister apologised to India on behalf of the nation, and offered generous compensation to the families of the killed and injured soldiers. Crucially, Islamabad also detained (but did not agree to extradite) a number of high-profile Islamic extremists (including the founder of *Lashkar-e-Taiba*, Hafiz Saeed). The rogue Pakistani commander himself had died in a shootout with Pakistani special forces as part of an immediate large-scale crackdown on Islamist elements within Pakistani society. Because of these steps, coupled with heavy and sustained international support and pressure to avert a full-blown nuclear war, New Delhi resisted the pressure by certain segments to retaliate further.

But although the loss of life was limited due to the conventional nature of the weapon and the relatively sparsely-populated nature of the terrain, sentiments previously voiced by senior Bharatiya Janata Party (BJP) officials over attacks emanating from Pakistani soil such as '*ek daant ke lie poore jabade*' (for one tooth, the complete jaw) found a willing audience in India's rightly outraged population. Tub-thumping nationalist pundits were able to use mainstream media elements to promote a kind of jingoism that was even more extreme than the type seen in previous years over hyped-up 'surgical strikes' and other retaliatory measures. This, combined with the government's perceived 'inaction', meant, however, that India's Muslim community (standing at over 180 million people) began to bear the brunt of public anger. Vigilante reprisal attacks and large-scale riots began in volatile northern Indian cities like Aligarh, and subsequently spread across the country.

The consequences

The failure to stop intermittent communal rioting had put India's secular and multi-faith democracy at risk. The country's Muslims, who now numbered over 200 million, had become even more marginalised and disenfranchised. As a result, pockets of armed resistance spread beyond areas which had previously witnessed jihadist-inspired violence. India was due to soon overtake Indonesia as the country with the world's largest Muslim population, and the creeping radicalisation of an already disadvantaged minority community only sought to aggravate aggressive majoritarian attitudes. A Hindu nationalist agenda was finally consolidated after successes by hardliners in a number of key regional elections, which allowed divisive figures (such as Yogi Adityanath) to implement a number of policies. Although there had been a drop in foreign direct investment (FDI) in India immediately after the crisis, and the country witnessed a slowdown in its impressive economic growth, foreign companies and governments began shortly afterwards to re-invest. Seemingly, India's huge and growing market allowed international actors to turn a blind eye to negative social and political developments.

Regional integration efforts (which were already practically dead due to the India-Pakistan rivalry) had totally collapsed, with SAARC being officially disbanded in 2021. India's military wielded increased influence in politics and underwent a huge ten-year modernisation programme. The economy was thus re-organised to allow for a massive re-direction of financial resources to the defence budget. This starved funds for areas such as the already dire educational sector, with the knock-on effect of increasing India's bloated unemployment rates. The quality of life for many Indians, who already in 2022 became the world's largest population, began to worsen as underfunded challenges such as pollution and other health issues took their toll.

One unexpected consequence was that New Delhi abandoned its more neutral stance in world affairs and formed a loose military alliance with the US, which was willing to overlook the country's worrying domestic developments. Yet this fact, combined with still simmering territorial disputes and arguments with China over control of water resources in the Tibetan Plateau, meant that a serious military conflict with Beijing became a serious possibility.

Pakistan, meanwhile, continued to suffer increased militantism in its tribal areas, as well as growing separatism in regions such as Balochistan. The rump of Pakistan which was still under full government control, centred along the Punjab, while not a theocracy, was ruled by a hardline military dictatorship strongly influenced by fundamentalist Islamist beliefs. China had also joined Pakistan's side as a more formal ally in order to cement a strategic alliance which allowed Beijing to complete its new network of economic corridors, as well as see off growing geo-political competition from India.

Where did it all go wrong?

Although a number of official risk-reduction and confidence-building measures had been in place before the incident, such as a missile launch warning accord and a military-to-military hotline, Pakistan remained at risk of rogue extremist army elements launching a conventional (or even nuclear) attack or leaking nuclear materials or data to terrorists or criminals. Moreover, despite the importance attached to the country's nuclear weapons, Islamabad had taken a number of risks with its nuclear arsenal: out of fear of the weapons being captured, unprotected unmarked vehicles had been used to transport nuclear weapons around the country, for instance. And although numerous command and control aspects had been addressed by the Pakistani authorities, the proliferation of tactical nuclear weapons – in addition to an increased decentralisation of command and maintaining weapons systems in a deployed status – had allowed for the doubt and fear of a nuclear attack to dominate the initial stages of the crisis.

The repeated refusal of Pakistan to root out extremist elements in both its educational and military sectors had allowed fundamentalist Islamic views to permeate through all layers of society – including business elites, government officials and top military brass. The military had undergone a large-scale Islamisation process since the General Zia-ul-Haq's coup in 1977, which in addition to softer elements like banning alcohol in the officers' mess, also led to the armed forces adopting military doctrines which included elements of ethnic superiority of Pakistani Muslims over Indian Hindus. This process was mirrored in the civilian sector: the failure to repeal the much-abused blasphemy law, for instance, was a high-profile example which only emboldened hardliners.

Increasingly assertive strands of Hindu nationalism, coupled with the unwillingness (or even inability) of Indian Prime Minister Narendra Modi to rein in reactionary elements within his own party – or groups linked to it like *Rashtriya Swayamsevak Sangh* (RSS) – had polarised Indian society. Externally, it also angered Muslims around the world, including elements within the Pakistani armed forces. Moreover, the implosion of the once-mighty Congress Party over its unwillingness to break with dynastic politics had left the BJP government without a strong political opposition in both upper and lower houses.

Finally, the violent responses meted out by the Indian armed forces and paramilitary groups to protesters in Kashmir in early 2017 only stoked further localised resistance, as well as public indignation across the Line of Control (LoC) in Pakistan. The continued refusal to modify Armed Forces (Special Powers) Act (AFSPA) – which had long been blamed as a facilitator of abuse – had a similar effect. In a spiralling vicious circle, violence in Kashmir began to return to the levels witnessed in the 1990s, again compounding the issue of radicalisation and tensions on both sides of the LoC.

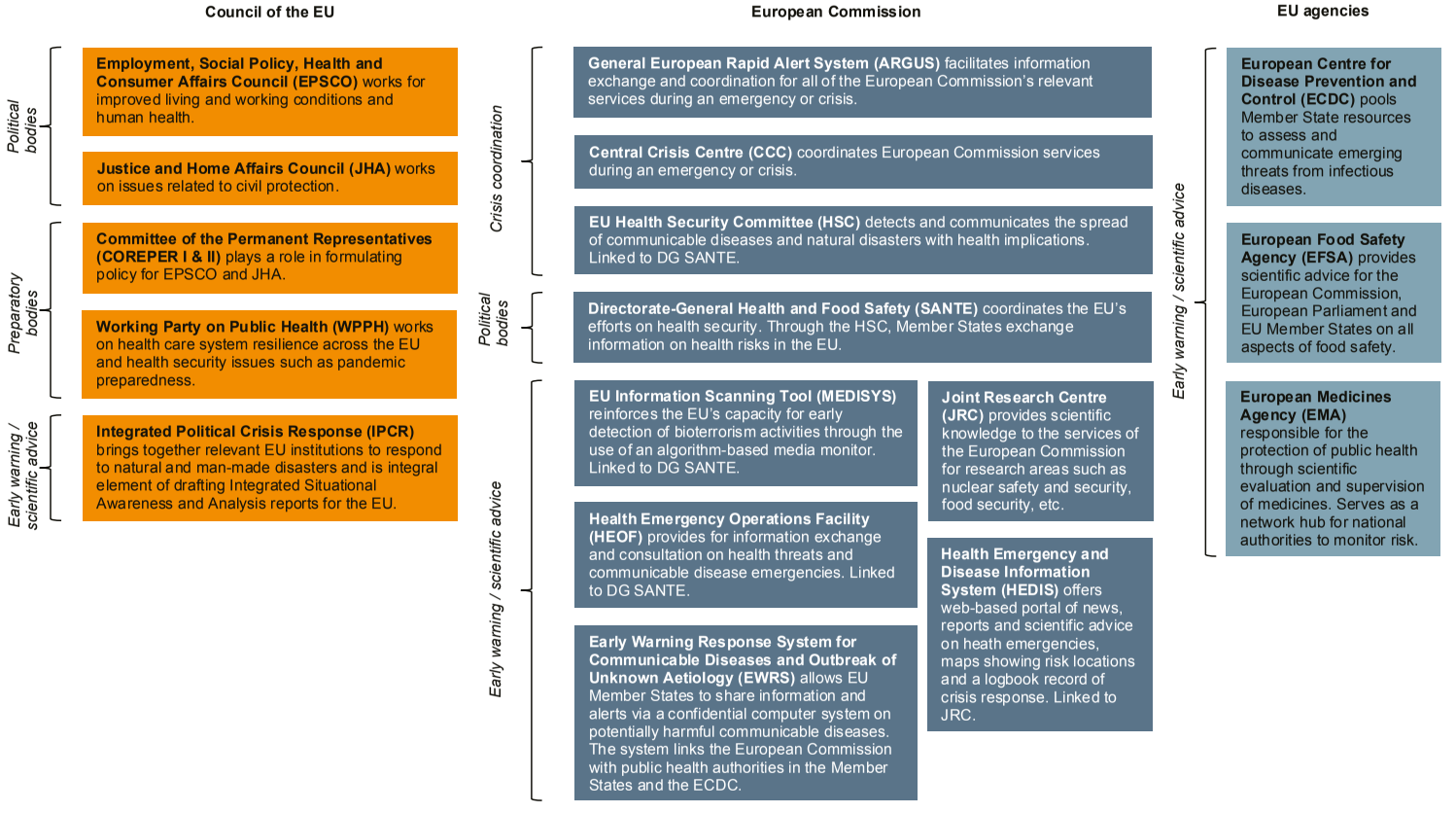
ANNEX

Having now read the grey swan scenarios in this report, the reader will be fully acclimatised to (and perhaps slightly shocked by) the world that the 'red team' have created. But what does the 'blue team' look like? Which actors and mechanisms would be called upon to provide an EU response?

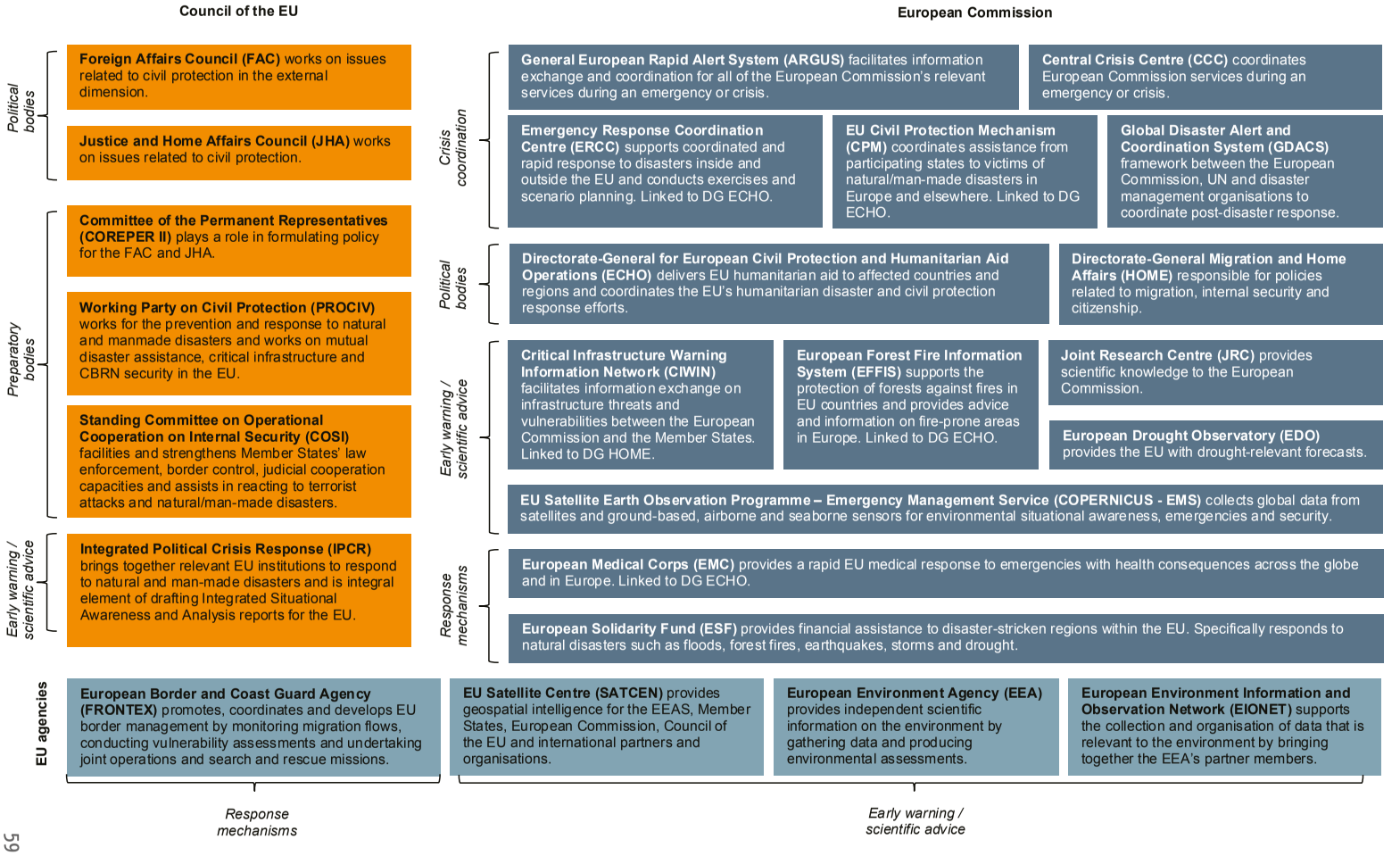
The purpose of this annex is to outline some of the major political and preparatory bodies, response and planning mechanisms and early-warning tools and networks that could possibly be available to the EU when a crisis and/or 'grey swan' situation occurs. In short, the set of 'maps' presented here aims to provide a cursory look at the 'blue team' that would likely be involved in any EU response to a crisis. The maps categorise different actors and tools by the potential role they would assume during a crisis (i.e. early-warning, planning, political decision-making, etc). The 'blue team' maps presented in the following pages cover a range of potential crisis areas including: public health, natural disasters, external crises, CBRN, terrorism, infrastructure and cyber. This is, of course, not an exhaustive list of the types of grey swan situations that could emerge.

The 'blue team' maps are not designed to offer an exhaustive list of actors and mechanisms, as they are simply intended to show the institutional complexity that is involved in EU crisis prevention and response. Furthermore, the maps do not seek to engage in organogram-style levels of hierarchy. While the institutional affiliation of each actor and mechanism is denoted by a colour, the individual boxes are purposefully unconnected as the challenge facing any decision-maker would be how to bring together and effectively combine all of these seemingly disparate prevention/response tools.

PUBLIC HEALTH AND DISEASE



NATURAL DISASTERS/CIVIL PROTECTION



EXTERNAL CRISES

Council of the EU

Political bodies

Foreign Affairs Council (FAC) works on issues related to civil protection in the external dimension.

Political and Security Committee (PSC) monitors the international situation, defines policies relevant for EU external action and exercises political control over EU crisis response.

Preparatory bodies

Committee of the Permanent Representatives (COREPER II) plays a role in formulating policy for the FAC and JHA.

Committee for Civilian Aspects of Crisis Management (CIVCOM) advises the PSC on all civilian aspects of crisis management. It plans and makes recommendations for new CSDP missions and is responsible for developing civilian capabilities.

Working Party of Foreign Relations Counsellors (RELEX) deals with legal, financial and institutional issues of the CFSP.

Politico-Military Group (PMG) ensures all preparatory work for the PSC for all political aspects of EU military/civilian operations. It also facilitates all relevant information exchange between Member States.

EU Military Committee (EUMC) is the highest military body responsible for advice and recommendations on all military matters.

EU agencies

Response

European Border and Coast Guard Agency (FRONTEX) coordinates EU border management by monitoring flows, conducting assessments and undertaking operations.

Early warning

EU Satellite Centre (SATCEN) provides geospatial intelligence for the EEAS, Member States, European Commission, Council of the EU and international partners and organisations.

European Commission

Political bodies

Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) delivers EU humanitarian aid to affected countries and regions and coordinates the EU's humanitarian disaster and civil protection response efforts.

Directorate-General European Neighbourhood Policy and Enlargement Negotiations (NEAR) responsible for all aspects of the EU's neighbourhood policy and the delivery of the ENI.

Directorate-General Migration and Home Affairs (HOME) responsible for policies related to migration and asylum policy, internal security and citizenship.

Crisis coordination

Emergency Response Coordination Centre (ERCC) supports coordinated and rapid response to disasters inside and outside the EU and conducts exercises and scenario planning. Linked to DG ECHO.

Response mechanisms

European Medical Corps (EMC) provides rapid medical response to emergencies with health consequences across the globe. Linked to DG ECHO.

European Neighbourhood Instrument (ENI) supports economic development, security and migration and mobility in EU partner countries through financial aid.

Emergencies Support Instrument (ESI) supports humanitarian needs of refugees located in the EU through financial support.

Instrument contributing to Stability and Peace (IcSP) focuses on delivering financial aid for crisis response, preparedness and conflict prevention as part of the EU's external action.

European External Action Service

Crisis coordination

Crisis Response System (CRS) ensures coherence between EU actors for the prevention and response to external crises that affect EU assets and/or persons in a third country.

Crisis Response and Operational Coordination Department (CROCD) responsible for activating CRS and mobilising actors and instruments across the EU system for external crises and consular emergencies.

Prevention of Conflicts, Rule of Law, Security Sector Reform, Integrated Approach, Stabilisation and Mediation (PRISM) responsible department within the EEAS for range of crisis-related tasks and serves as hub of information exchange between Member States and international organisations.

Security Policy (SECPOL) responsible for crisis issues such as disarmament, non-proliferation, counter-terrorism, space policy and sanctions.

Planning

Military Planning and Conduct Capability (MPCC) commands and controls all military CSDP non-executive missions.

Joint Support Coordination Cell (JSCC) ensures synergies between the MPCC and CPCC.

Civilian Planning and Conduct Capability (CPCC) responsible for ensuring the planning and conduct of civilian missions conducted under the CSDP.

Crisis Management and Planning Directorate (CMPD) responsible for politico-strategic planning of civilian and military CSDP operations.

EU Military Staff (EUMS) responsible for providing the EEAS with all aspects of military advice especially with regard to EU operations and missions.

Early warning

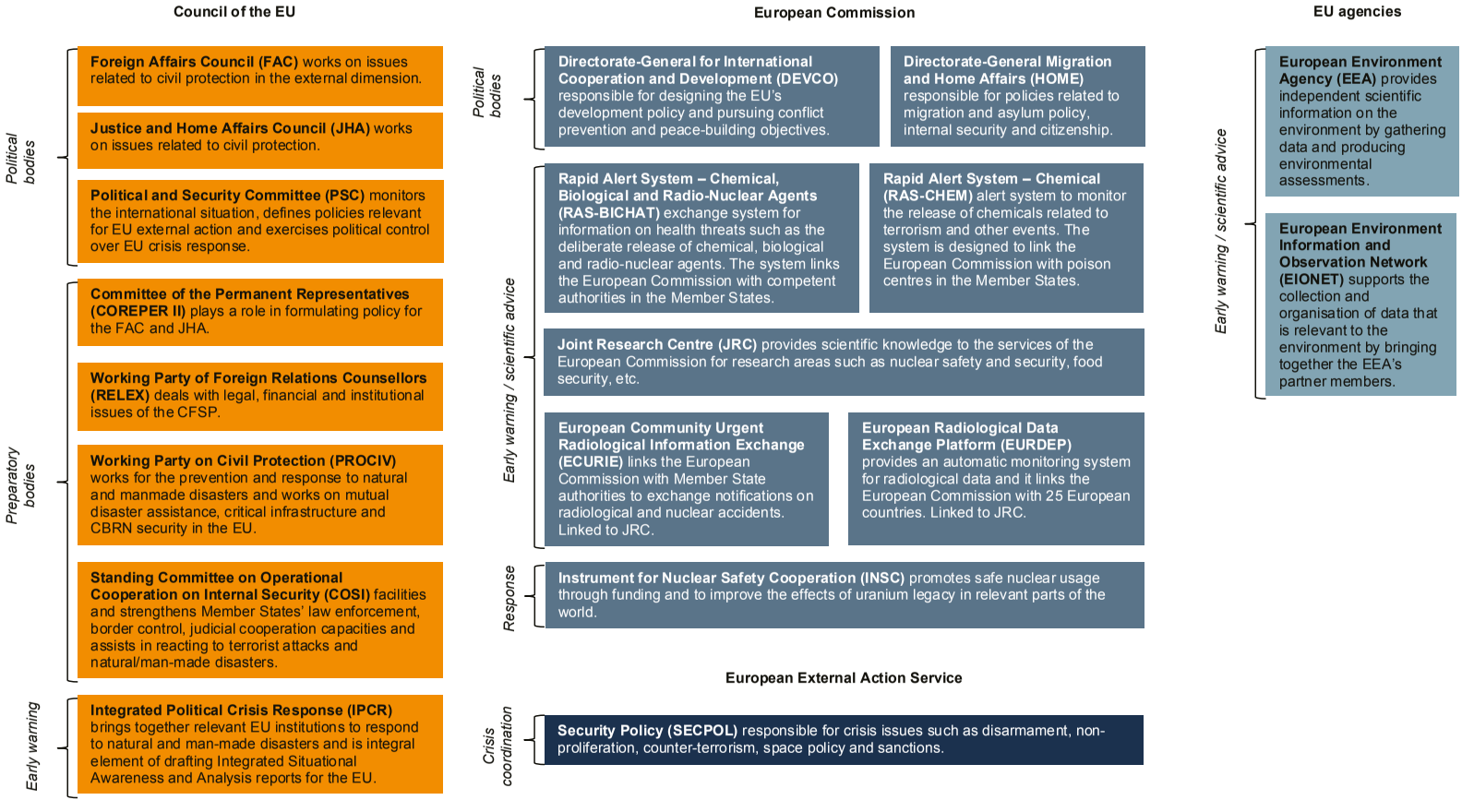
EU Intelligence and Situation Centre (INTCEN) serves as the EU's civilian intelligence-gathering hub and produces intelligence assessments based on EU Member States' intelligence and security services.

Single Intelligence Analysis Capacity (SIAC) coordinates intelligence gathering efforts between INTCEN and the EUMS intelligence directorate.

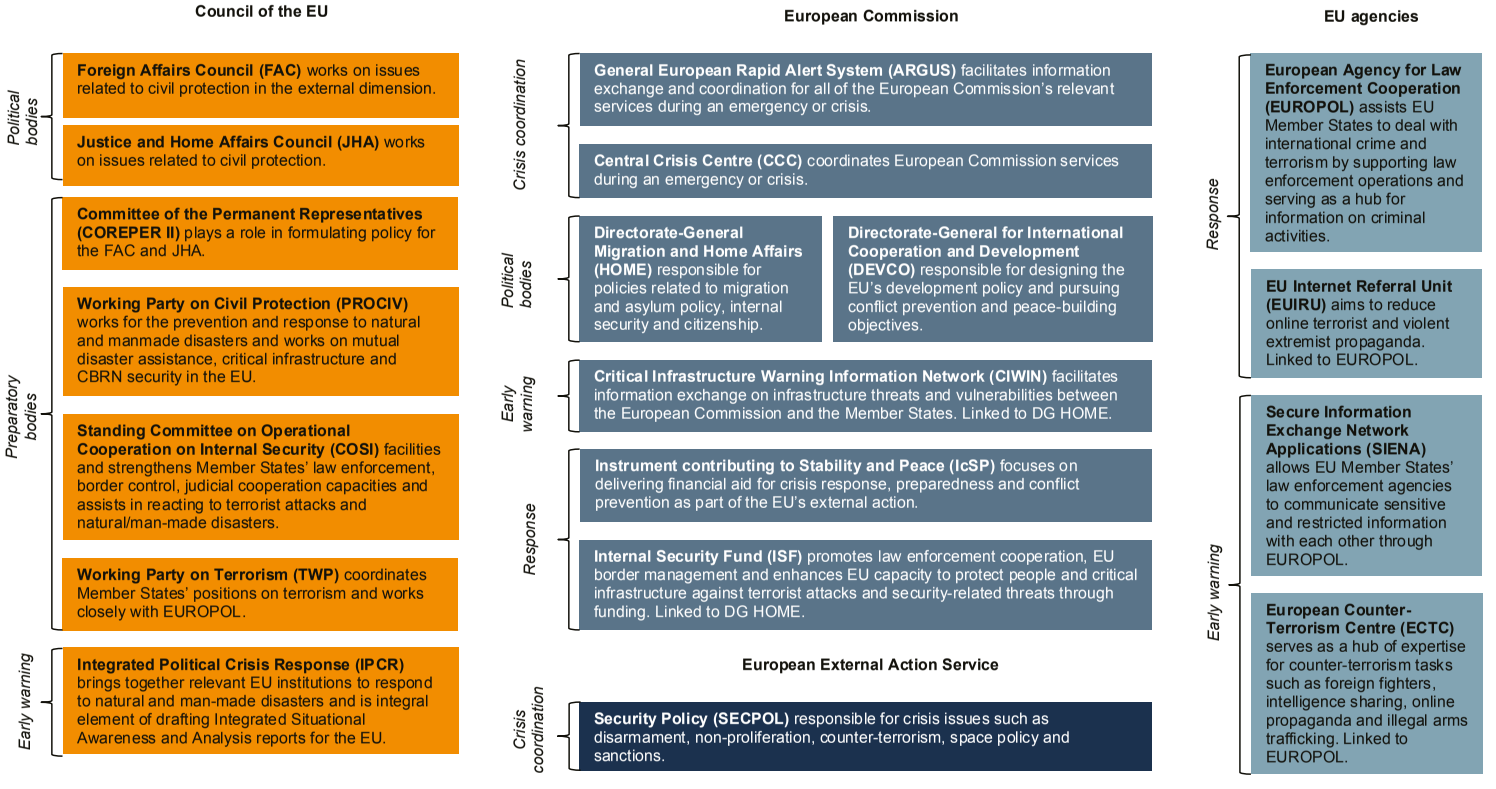
EU Delegations (EUDEL): the EU's network of diplomatic delegations and offices are located around the world.

Departments (DEPT) for regions and countries play a role in information gathering for crisis situations.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENCE (CBRN)



TERRORISM


Council of the EU
Political bodies
Foreign Affairs Council (FAC) works on issues related to civil protection in the external dimension.
Justice and Home Affairs Council (JHA) works on issues related to civil protection.
Preparatory bodies
Committee of the Permanent Representatives (COREPER II) plays a role in formulating policy for the FAC and JHA.
Working Party on Civil Protection (PROCIV) works for the prevention and response to natural and manmade disasters and works on mutual disaster assistance, critical infrastructure and CBRN security in the EU.
Standing Committee on Operational Cooperation on Internal Security (COSI) facilities and strengthens Member States' law enforcement, border control, judicial cooperation capacities and assists in reacting to terrorist attacks and natural/man-made disasters.
Working Party on Terrorism (TWP) coordinates Member States' positions on terrorism and works closely with EUROPOL.
Early warning
Integrated Political Crisis Response (IPCR) brings together relevant EU institutions to respond to natural and man-made disasters and is integral element of drafting Integrated Situational Awareness and Analysis reports for the EU.
European Commission
Crisis coordination
General European Rapid Alert System (ARGUS) facilitates information exchange and coordination for all of the European Commission's relevant services during an emergency or crisis.
Central Crisis Centre (CCC) coordinates European Commission services during an emergency or crisis.
Political bodies
Directorate-General Migration and Home Affairs (HOME) responsible for policies related to migration and asylum policy, internal security and citizenship.
Directorate-General for International Cooperation and Development (DEVCO) responsible for designing the EU's development policy and pursuing conflict prevention and peace-building objectives.
Early warning
Critical Infrastructure Warning Information Network (CIWIN) facilitates information exchange on infrastructure threats and vulnerabilities between the European Commission and the Member States. Linked to DG HOME.
Response
Instrument contributing to Stability and Peace (IcSP) focuses on delivering financial aid for crisis response, preparedness and conflict prevention as part of the EU's external action.
Internal Security Fund (ISF) promotes law enforcement cooperation, EU border management and enhances EU capacity to protect people and critical infrastructure against terrorist attacks and security-related threats through funding. Linked to DG HOME.
European External Action Service
Crisis coordination
Security Policy (SECPOL) responsible for crisis issues such as disarmament, non-proliferation, counter-terrorism, space policy and sanctions.
EU agencies
Response
European Agency for Law Enforcement Cooperation (EUROPOL) assists EU Member States to deal with international crime and terrorism by supporting law enforcement operations and serving as a hub for information on criminal activities.
EU Internet Referral Unit (EUIRU) aims to reduce online terrorist and violent extremist propaganda. Linked to EUROPOL.
Early warning
Secure Information Exchange Network Applications (SIENA) allows EU Member States' law enforcement agencies to communicate sensitive and restricted information with each other through EUROPOL.
European Counter-Terrorism Centre (ECTC) serves as a hub of expertise for counter-terrorism tasks such as foreign fighters, intelligence sharing, online propaganda and illegal arms trafficking. Linked to EUROPOL.

INFRASTRUCTURE

Council of the EU

Political bodies

Justice and Home Affairs Council (JHA) works on issues related to civil protection.

Transport, Telecommunications and Energy Council (TTE) works to improve trans-European infrastructure related to aviation, maritime, energy and telecommunications.

Preparatory bodies

Committee of the Permanent Representatives (COREPER II) plays a role in formulating policy for JHA.

Committee of the Permanent Representatives (COREPER I) plays a role in formulating policy for TTE.

Standing Committee on Operational Cooperation on Internal Security (COSI) facilities and strengthens Member States' law enforcement, border control, judicial cooperation capacities and assists in reacting to terrorist attacks and natural/man-made disasters.

Working Party on Civil Protection (PROCIV) works for the prevention and response to natural and manmade disasters and works on mutual disaster assistance, critical infrastructure and CBRN security in the EU.

Early warning

Integrated Political Crisis Response (IPCR) brings together relevant EU institutions to respond to natural and man-made disasters and is integral element of drafting Integrated Situational Awareness and Analysis reports for the EU.

European Commission

Political bodies

Directorate-General Migration and Home Affairs (HOME) responsible for policies related to migration and asylum policy, internal security and citizenship.

Directorate-General Energy (ENER) responsible for policies related to energy infrastructure.

Directorate-General Mobility and Transport (MOVE) responsible for policies related to transport infrastructure.

Early warning

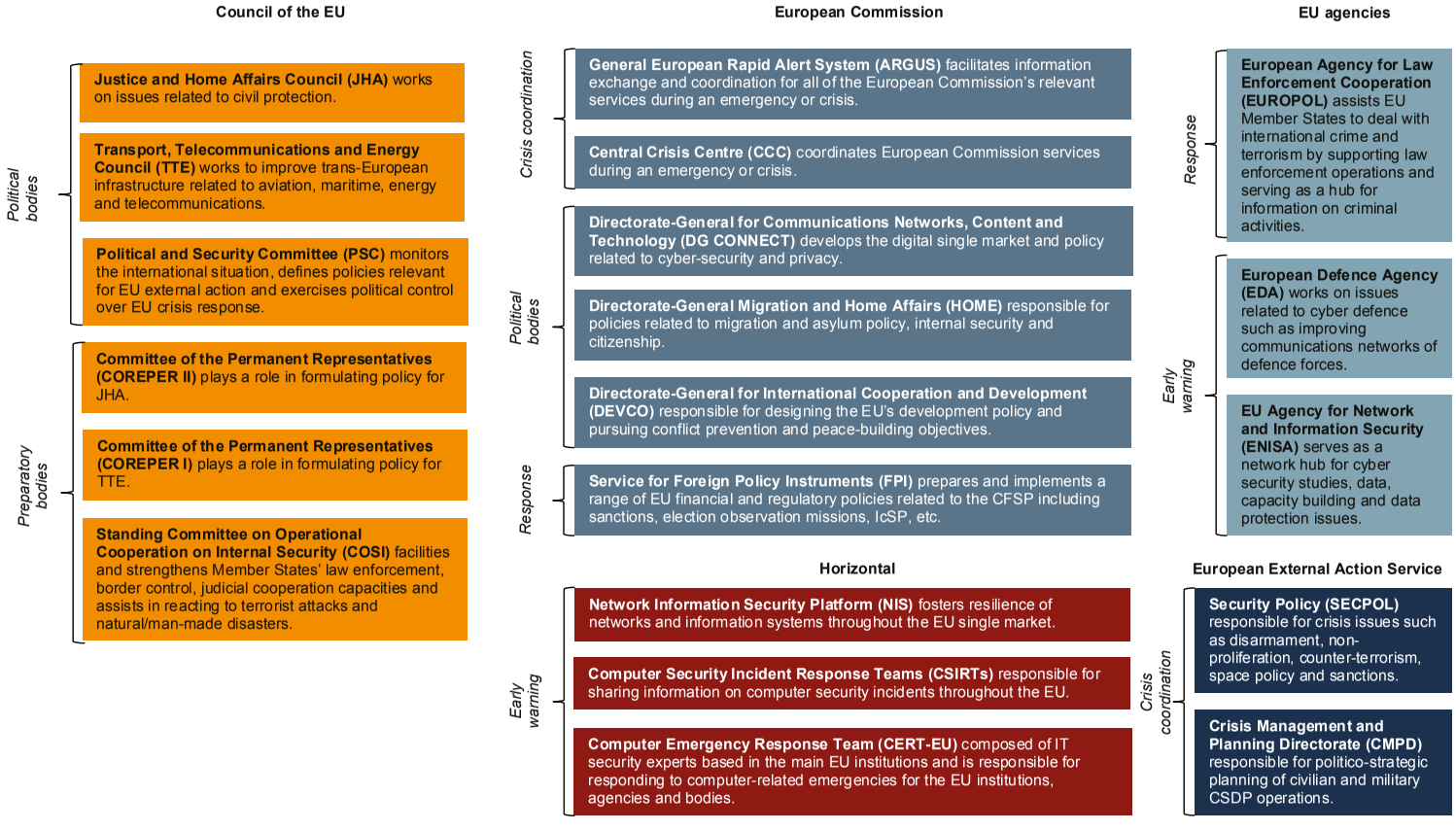
Critical Infrastructure Warning Information Network (CIWIN) facilitates information exchange on infrastructure threats and vulnerabilities between the European Commission and the Member States. Linked to DG HOME.

EU agencies

Early warning

European Maritime Safety Agency (EMSA) provides technical assistance to the European Commission and Member States on maritime safety, ship pollution and maritime security.

CYBER


Council of the EU
Political bodies
Justice and Home Affairs Council (JHA) works on issues related to civil protection.
Transport, Telecommunications and Energy Council (TTE) works to improve trans-European infrastructure related to aviation, maritime, energy and telecommunications.
Political and Security Committee (PSC) monitors the international situation, defines policies relevant for EU external action and exercises political control over EU crisis response.
Preparatory bodies
Committee of the Permanent Representatives (COREPER II) plays a role in formulating policy for JHA.
Committee of the Permanent Representatives (COREPER I) plays a role in formulating policy for TTE.
Standing Committee on Operational Cooperation on Internal Security (COSI) facilities and strengthens Member States' law enforcement, border control, judicial cooperation capacities and assists in reacting to terrorist attacks and natural/man-made disasters.
European Commission
Crisis coordination
General European Rapid Alert System (ARGUS) facilitates information exchange and coordination for all of the European Commission's relevant services during an emergency or crisis.
Central Crisis Centre (CCC) coordinates European Commission services during an emergency or crisis.
Political bodies
Directorate-General for Communications Networks, Content and Technology (DG CONNECT) develops the digital single market and policy related to cyber-security and privacy.
Directorate-General Migration and Home Affairs (HOME) responsible for policies related to migration and asylum policy, internal security and citizenship.
Directorate-General for International Cooperation and Development (DEVCO) responsible for designing the EU's development policy and pursuing conflict prevention and peace-building objectives.
Response
Service for Foreign Policy Instruments (FPI) prepares and implements a range of EU financial and regulatory policies related to the CFSP including sanctions, election observation missions, IcSP, etc.
EU agencies
Response
European Agency for Law Enforcement Cooperation (EUROPOL) assists EU Member States to deal with international crime and terrorism by supporting law enforcement operations and serving as a hub for information on criminal activities.
Early warning
European Defence Agency (EDA) works on issues related to cyber defence such as improving communications networks of defence forces.
EU Agency for Network and Information Security (ENISA) serves as a network hub for cyber security studies, data, capacity building and data protection issues.
Horizontal
Early warning
Network Information Security Platform (NIS) fosters resilience of networks and information systems throughout the EU single market.
Computer Security Incident Response Teams (CSIRTs) responsible for sharing information on computer security incidents throughout the EU.
Computer Emergency Response Team (CERT-EU) composed of IT security experts based in the main EU institutions and is responsible for responding to computer-related emergencies for the EU institutions, agencies and bodies.
European External Action Service
Crisis coordination
Security Policy (SECPOL) responsible for crisis issues such as disarmament, non-proliferation, counter-terrorism, space policy and sanctions.
Crisis Management and Planning Directorate (CMPD) responsible for politico-strategic planning of civilian and military CSDP operations.

QN-AF-17-005-EN-N

European Union Institute for Security Studies
100, avenue de Suffren | 75015 Paris | France | www.iss.europa.eu

ISBN 978-92-9198-625-5