EUROPEAN
COUNCIL
ON FOREIGN
RELATIONS
ecfr.eu

POLICY BRIEF

IRON NET: DIGITAL REPRESSION IN THE MIDDLE EAST AND NORTH AFRICA

James Lynch

June 2022

SUMMARY

- Governments across the world have powerful digital tools to control and repress their populations, ranging from spyware and social media manipulation to facial recognition technology and mass surveillance.
- Activists are working to protect themselves from such tools, but this is not a fair fight.
- Saudi Arabia and the UAE are the leading exponents of digital authoritarianism in the Middle East.
- The two states have intensified their collaboration with China and Israel to gain greater access to advanced technologies.
- The EU has responded to concerns about the risks of new technologies with a raft of regulations on digital markets and services, artificial intelligence, and technology exports.
- The fact that European governments have been targeted, and implicated, in NSO Group's Pegasus scandal should sound the alarm about the global threat of digital authoritarianism.
- The EU should treat the threat as an urgent security and political concern.

Introduction

In April 2021, Malcolm Bidali, a Kenyan security guard living in Doha, opened his Twitter account to find that someone had sent him a link to a Human Rights Watch report about migrant workers. Bidali was using an anonymous account, @noaharticulates, to blog about his life and document the daily exploitation and abuse that he and his fellow workers experienced. His account, which only had a few hundred followers, had just begun to attract interest both from foreign readers and young Qataris who appreciated his frank, unflinching account of the reality he and his colleagues confronted every day.

The link did not work. But it was never meant to: it was a phishing link designed to reveal the true identity of @noaharticulates. A week later, Bidali was arrested at his labour camp by State Security officers. After a month in solitary confinement and a campaign for his release by students in Qatar, he was deported to Kenya with a hefty fine for publishing "false news with the intent of endangering the public system of the state". And there ended the career of Qatar's first – and, so far, only – migrant worker blogger. A year before the 2022 Men's Football World Cup, the build-up to which had been characterised by international concern about the abuse of migrant workers, the Qatari state had used a relatively simple technical measure to snuff out a perceived threat.

For much of the world's population, the digital realm has become central to the human experience. Yet access to information and essential services is often mediated by digital platforms, with or without users' knowledge. This means that the governments, businesses, or individuals who dominate the digital realm have the potential to gain control over the public sphere. There is now little trace of the widespread optimism that once defined public views of the digital revolution. Far from being a prelude to liberation, this revolution has increasingly allowed states to exercise control and even engage in repression. As Egyptian technologist, blogger, and activist Alaa Abd el-Fattah argued in a 2017 essay written in Tora Prison: "the authorities have decided: meaning is dangerous, defending it is a crime, and its proponents are enemies." Civil society organisations have strained to find ways to protect themselves from digital attacks, bypass state censorship, or challenge disinformation – but this has not proved to be a fair fight.

It is nothing new for governments to repress their populations or seek to control the flow of information – authoritarians have always wanted to stop the spread of dangerous ideas and replace them with official narratives. And they have always sought information about citizens by monitoring their activities. The difference now is that governments have an astonishing array of tools with which to achieve these goals – ranging from spyware to facial recognition technology and mass surveillance. And they can use these tools with little concern that they will be held accountable for doing so.

The human costs of digital authoritarianism are evident across the world, but particularly in the Middle East and North Africa – where the rule of law was, at best, under severe strain even before the digital revolution. Saudi Arabia and the United Arab Emirates have invested heavily in new technologies, including through intensified collaboration with China and Israel, as part of an effort to become digital superpowers. The lack of an international consensus on how such tools should be governed has created a fractured landscape of competing principles and multilateral initiatives that digital authoritarians often exploit.

European policymakers are rightly concerned about these developments. As this author argued in 2021, governments in the Middle East and North Africa are becoming even more authoritarian. The digital dimension of authoritarianism is central to this trend. Given that repeated human rights violations and a lack of accountability frequently lead to societal breakdown, the European Union seems misguided in its reliance on authoritarians to guarantee stability and security in its southern neighbourhood.

EU policy should treat digital authoritarianism in the region as a significant security and political concern. But there is no sign that it is doing so. As a 2021 European Parliament research paper put it, the EU "still has to decide whether tackling digital repression is a core geopolitical interest at the highest political level".

Authoritarian states' use of surveillance technology shows why this is a problem. Responding to the risks associated with digital technologies, the European Commission published in January 2022 a draft Declaration on European Digital Rights and Principles with the aim of creating a "human-centred, secure, inclusive, and open digital environment, where no one is left behind". The draft includes the principle that "no one shall be subjected to unlawful online surveillance or interception measures". Yet it will be challenging to adhere to this principle in Europe. Trade in surveillance technology – including that involving European companies – has spun out of control. For instance, Morocco and the UAE reportedly targeted the communications of French President Emmanuel Macron and British Prime Minister Boris Johnson respectively.

Until 2020, Israeli company NSO Group had an office in Cyprus – which was a hub for surveillance consultants – and promoted its products at UK defence fairs while under investigation by the FBI and facing a lawsuit for hacking brought by WhatsApp. The EU has declined to sanction the company. The United States has restricted export licences involving NSO Group (a move that Israel is lobbying to reverse) but, in the EU, such decisions are made by member states.

The EU is poorly suited to dealing with the graduated, subtle trend towards digital repression (in contrast to more urgent threats to democracy and human rights, such as Russia's war on Ukraine). The International Institute for Democracy and Electoral Assistance has reported "a deep and dangerous cleavage in the EU's internal fundamental consensus on liberal democratic values", with Hungary and Poland transitioning into "soft authoritarianism".

Governments in Hungary, Poland, Germany, and Spain have all been accused of using NSO Group's Pegasus technology to target domestic critics, including journalists and politicians. The company told the European Parliament in June 2022 that at least five EU countries had used Pegasus. Meanwhile, the company's technology has played a critical role in engendering and cementing relationships between Israel and authoritarian states around the world, including Saudi Arabia, the UAE, India, and Hungary.

This paper focuses on some of the key forms of digital repression in the Middle East and North Africa, and their implications for deepening Israeli-Gulf links and Chinese digital diplomacy. It analyses the main ways in which Europeans are currently responding to these trends – including through regulation and diplomacy – and makes recommendations for how they should address the challenges posed by spyware, artificial intelligence, and the protection of civil society.

Threat ctrl, social ctrl

In hindsight, rapid technological advances had a transformative impact between 2009 and 2012. Governments everywhere from Tehran and Cairo to Manama and Damascus appeared to be digital novices as they wrestled with the increasing availability of smartphones and the development of social media platforms. They seemed unable to respond effectively as activists and young people freely shared information with one another and the wider world, circumventing traditionally powerful state-controlled media. Some analysts have made the compelling argument that overexcited commentators (particularly those in the West) undervalued the contribution of offline mobilisation and organising, and that tech companies used the 2011 uprisings to promote a positive narrative about their contributions to society. But there is no doubt that new technologies had a huge impact on political organisation. And they continue to do so: just as protests in the Arab-speaking world in the early 2010s were influenced by Twitter and Facebook, those in Myanmar, Hong Kong, and Belarus more recently have been shaped by Telegram, WhatsApp, and Signal.

However, the resulting technological pushback from governments across the Middle East and North Africa has been swift and transformative in its own way. As analyst James Shires argues, the "ambiguity, imprecision and multivalence" of the term "cybersecurity" – particularly the lack of consensus about what constitutes a legitimate security threat in the digital domain – has helped authoritarians legitimise various strategies for achieving their political goals. These strategies focus on everything from "negative control" to "proactive co-option". The former involves throttling the flow of critical or accurate information and silencing online irritants, while the latter is designed to shape narratives and create accepted truths, using massive digital data sets to identify emerging threats and opportunities.

Threat control: Online crackdowns and censorship

After the shock of the Arab uprisings, governments across the region introduced new laws and policies to place the same restrictions on online discourse as applied to the public statements of journalists and opposition leaders. Under the repressive and often interchangeable cyber-crime laws that swept the region in the early 2010s, online commentary on almost any topic could be an imprisonable offence if the government deemed it a threat to state interests or public security such as "support for terrorism". States also deliberately conflated legitimate political criticism with "fake news" and other forms of disinformation, allowing them to portray legal persecution as a defence of freedom of expression.

Governments arrested swathes of activists, journalists, and ordinary Twitter users under these new rules. In 2018 an Egyptian court gave Amal Fathy a two-year prison sentence for posting a Facebook video about her experience of being sexually harassed – on the charge of "using a website to promote ideas calling for terrorist acts". A Jordanian teacher who used his Facebook account to peacefully criticise his government was seized by masked UAE security officers as he was walking with his children in 2020. He was held incommunicado and handed a ten-year sentence for "acts against a foreign state". Police and judicial harassment became commonplace, affecting all kinds of social media users, ranging from royals in Kuwait and internet activists in Oman to journalists in Tunisia.

Authoritarian governments have gone to great lengths to identify critics who operate anonymously: a 2018 FBI complaint accuses three men of working for Saudi Arabia to penetrate Twitter's Californian offices, with the aim of passing confidential information on thousands of users to the Saudi authorities. Abdulrahman al-Sadhan, arrested in 2018 and sentenced to 20 years in prison followed by a 20-year travel ban, was reportedly identified by the Saudi authorities due to this security breach at Twitter. He allegedly used an anonymous account to criticise the government's economic policies.

Authoritarian governments have also used their control over telecommunications networks to block unwelcome communications and other forms of information, targeting VPN users and encrypted VoIP apps that are designed to prevent surveillance. The UAE briefly lifted its restrictions on WhatsApp and Skype for international visitors to Expo 2020, but has otherwise banned calls on these services for years. Authoritarians liberally block websites they deem threatening. Syria is among the most censored internet environment in the world, a situation exacerbated by international sanctions – which push some foreign sites to restrict their own services there. Governments can also ask search engines and other platforms to remove specific content: countries with little internet freedom make the most requests for content removal, especially for reasons such as "government criticism" and "national security".

Instagram moderators report that the Iranian authorities offer bribes of between €5,000 and €10,000 to remove the accounts of critical journalists and activists. The Jordanian authorities have used a range of regulatory and technical tools to restrict many types of content and services, including Arabic LGBT+ websites and the entire Facebook Live service during protests. In extreme cases, governments simply block internet access for some or all of the population. Military leaders in Sudan shut down the internet immediately after launching a coup in late 2021. In May this year, Iran blocked almost all internet access in Khuzestan province, which was witnessing mass protests against rising food prices and a bloody crackdown. Foreign companies involved in providing mobile and internet services can find themselves accused of complicity in such shutdowns. France Telecom and UK firm Vodafone famously implemented the "kill-switch" at the request of Hosni Mubarak's government in 2011, at the height of anti-regime protests in Egypt.

Social control: Re-establishing the state's grip on dominant narratives

As well as cracking down on supposedly threatening information or narratives, authoritarians aggressively impose their own narratives to shape public perceptions – often successfully. Where citizens across the region seek to draw attention to popular grievances or state failure, they can be overwhelmed by state-led communications campaigns, which pump out disinformation and fake news, often adopting a violent and misogynistic tone.

This process helps turn social media platforms into a hostile environment in which it is hard to distinguish between propaganda and genuine comments. The resulting lack of certainty creates distrust in the public sphere and has a chilling effect on users, leading many of them to abandon the platforms altogether. Women are particularly liable to be targeted: Dima Sadek, a journalist who was using her Twitter account to report on Lebanon's protests in 2019, was subjected to an intense, coordinated programme of online harassment, including the sharing of faked compromising photos – as a result of which her mother had a stroke. One European Parliament report refers to such tactics as a key part of the "next generation repression toolkit".

As analyst Marc Owen Jones points out, the UAE and Saudi Arabia are "digital superpowers" partly because of their investments in controlling the online agenda through a variety of means, including troll and bot armies, as well as astroturfing – the practice of creating the false impression that legitimate users are spontaneously supporting a cause.[1] Twitter has removed thousands of accounts linked to the Emirati and Saudi governments.

Authoritarians often use firms to run influence operations on social media. This is partly for reasons of efficiency and scale, but also to maintain plausible deniability about their involvement in such practices. In late 2019 Twitter announced that it was removing tens of thousands of inauthentic accounts linked to SMAAT, a Saudi public relations firm, for "amplifying messages favorable to Saudi authorities". Such accounts are used by governments across the region and are usually referred to as "bots". When they are coordinated around a single political goal – such as undermining protests in Algeria or defaming human rights defenders in Morocco – they are sometimes known as "electronic flies". At the time of his murder by agents of the Saudi state, *Washington Post* columnist Jamal Khashoggi was reportedly planning to launch "the bees", a network of activists who would coordinate their tweets to counter the narratives promoted by the Saudi crown prince's electronic flies.

Authoritarians' propaganda campaigns also usually involve the accounts of real people to help amplify the government's narrative. In some cases, these people reportedly work directly in concert with the authorities.

According to 7amleh, an NGO, "an institutionalized system" formed of "the Israeli government, government-operated non-governmental organizations (GONGOs) and online trolls" works to smear Palestinian human rights activists and organisations as "terrorists" or supporters of terrorism. Israel's cyber unit – which is modelled on similar bodies in the United Kingdom and France – has reportedly bombarded platforms with requests to remove online posts in support of Palestinian political causes, prompting YouTube and Instagram to do so. Such activity even led to the removal of content posted by the Palestinian government.

Facebook (now Meta) has acknowledged that it made errors in removing content related to the 2021 protests against the evictions of Palestinians from their homes in the Sheikh Jarrah district of Jerusalem. The company's oversight board recommended that it go further by commissioning an independent investigation into the episode. This investigation was under way as of late 2021, but its findings have not yet been made public.

States sometimes deploy coordinated inauthentic behaviour on social media internationally. The aim of this is often to delegitimise protest movements they perceive as a threat to regional stability or, equally, to undermine their adversaries by supporting – or appearing to support – anti-government protests. Middle Eastern powers may have learnt from the Kremlin's use of disinformation in Syria, which has effectively sowed distrust and division, disempowering legitimate activists. Egypt, the UAE, Saudi Arabia, and Turkey have all been implicated in information operations that use social media to shape perceptions of the conflict in Libya, while the Egyptian government has seemingly battled for online attention with external opponents backed by Qatar. During protests in Lebanon in 2019, influencers who apparently emerged from nowhere with large numbers of followers and who were promoted heavily by Saudi networks, began to introduce sectarian and anti-Iran narratives into the online political discourse – in an apparent attempt to counter demonstrators' message of unity between faiths.

Russia's information operations have generally received far more international attention than those of Middle Eastern states. However, some EU officials believe that disinformation emanating from the Middle East and North Africa poses increasing "threats to democratic political and policymaking processes" in Europe. Analysis by the European External Action Service indicates that actors other than Russia "have emerged to varying degrees as prominent disinformation threats". The European Parliament held hearings in 2021 into the threat that Saudi Arabia, the UAE, and Iran pose in this area. For example, Iranian-linked accounts have recently been removed by Meta for inauthentic behaviour related to calls for Scottish independence.

The prolonged Saudi-backed takeover of Newcastle United FC in 2020 and 2021 was intensely debated on social media by fans of the club – many of whom welcomed the acquisition – and critics of the takeover who considered it a dangerous example of "sportswashing". Analysts noticed a surge in real and seemingly fake Saudi-based accounts that supported the takeover and promoted Saudi interests and policies. "I would be very surprised if there wasn't some PR firm at the helm trying to coordinate this," said Jones.[2]

Threat control: Spyware and Israeli-Gulf collaboration

Until recently, the capacity to carry out targeted electronic surveillance was largely restricted to major powers whose intelligence agencies had developed in-house expertise. The proliferation of commercial surveillance and spyware packages has changed all that. In the early 2010s, Canadian NGO Citizen Lab revealed that several Arab governments were employing Italian firm Hacking Team to track the activities of their political opponents, human rights activists, and others. In 2016 Italy barred the company from exporting its products outside the EU but, by 2019, the owner of Hacking Team was marketing KRAIT. This surveillance tool, described by one researcher at Citizen Lab as "a match made in heaven for human rights abusers", can take over Android devices to surveil them without requiring their owners to click on a link.

Spyware has played a crucial role in authoritarian governments' efforts to crush social movements and human rights groups. At the height of President Abdel-Fattah al-Sisi's unprecedented crackdown on Egyptian civil society in 2016-2017, seven human rights groups – all of which were being investigated as part of Case 173, a notorious investigation by the authorities – were targeted 90 times in three months using sophisticated malware. This malware was crafted as shared documents that contained timely and relevant information, and that came from legitimate providers such as Google and Dropbox.

The UAE led the way in developing its own cyber-surveillance capacities, employing more than a dozen former employees of the US National Security Agency – who worked through Abu Dhabi-based cyber-security firm DarkMatter – in what was known as Project Raven. The team helped develop the Karma platform, which allowed them to hack into the iPhones of hundreds of activists, political leaders, and suspected terrorists in 2016 and 2017. Crucially, Karma – like KRAIT – does not require a target to click on a link sent to their device, a capability one Raven operative described as being "like Christmas". Their targets included Ahmed Mansoor, an Emirati activist then known as "the last human rights defender in the UAE", who was subsequently arrested by state security agents and handed a ten-year sentence for his activities on social media. Prior to his arrest, Mansoor told journalists that the discovery of the spyware on his phone was "as bad as someone encroaching in your living room, a total invasion of privacy, and you begin to learn that maybe you shouldn't trust anyone anymore". Three former US officials were prosecuted for violating US hacking laws and export controls in relation to the project. In 2019 the *New York Times* revealed that ToTok, a popular social media app, was actually a surveillance tool – the sole shareholder of ToTok was Group 42, an Abu Dhabi-based company chaired by Tahnoon bin Zayed Al Nahyan, the UAE's national security adviser.

Facing this onslaught, social movements and civil society networks have not merely been passive victims of repression: rather, they have strained to find ways of protecting themselves and bypassing censorship. Groups such as SMEX and 7amleh provide digital security services and advice across the Arabic-speaking world, while organisations based in the relative safety of Europe and North America – such as EFF, Access Now, and Amnesty's Security Lab – also provide technical guidance and support, as well as assistance with investigations. Advocacy groups such as the Heartland Initiative have begun to press technology investors to pay greater heed to the risks associated with cyber-security firms in their portfolios. Activists who have been hacked have also begun to seek legal routes to hold those responsible accountable: Loujain al-Hathloul, a Saudi women's rights activist who was jailed and tortured after being arrested in the UAE, has lodged a case against American executives at DarkMatter for their role in hacking her phone.

Nevertheless, even the most tech-savvy activists struggle to protect themselves: encryption technology has failed to keep up with hacking tools, as was chillingly demonstrated by the Pegasus revelations in 2021. Pegasus can penetrate a device with a "zero-click" attack, take complete control of a smartphone, and potentially leave without a trace. Among the 50,000 numbers that researchers into the tool accessed, they found 180 that belonged to journalists and many more that belonged to human rights defenders, academics, businesspeople, lawyers, doctors, union leaders, diplomats, politicians, and even heads of states. Pegasus was used to hack the devices of human rights activists across the Middle East and North Africa – including those working on abuses by the Bahraini state, documenting Israeli violations of Palestinians' rights, and defending Sahrawi rights. The tool gave the state unparalleled access to their activities and networks, as well as to their personal lives. As the EU data protection supervisor put it, Pegasus combined "a level of intrusiveness that is incomparable with what we have seen before, with features capable to render many of the existing legal and technical safeguards ineffective and meaningless".

Proponents of such technologies argue that while they may be misused in some cases, states have a legitimate use for spyware – countering criminal activity. Revelations about Pegasus have brought home the extent to which states themselves are at risk from cyber-surveillance technologies, making their proliferation an issue of national security as well as a human rights concern.

Pegasus was developed and marketed by NSO Group – which is one of several Israeli companies at the forefront of the cyber-surveillance industry. In 2011 the Israeli government published a national cyberspace strategy that set out its commitment to advance "Israel's status as a center for the development of information technologies" and "to work to encourage the cyber industry in Israel". The strategy bore fruit: in 2021 the Israeli cyber-security industry raised $8.8 billion in funding, with

Israeli companies accounting for one in three cyber-security unicorns (startups valued at over $1 billion) globally. In 2021 the value of Israel's cyber-security exports totalled $11 billion, roughly equal to that of its arms exports.

There is a well-established pathway from Israeli security entities, particularly the Israel Defense Force's elite Unit 8200, sometimes referred to as Israel's National Security Agency, to the private sector. One Israeli tech recruiter told *Haaretz* that, "serving in a tech division of military intelligence is the best shortcut there is to the business sector." A 2018 study found that 80 per cent of employees of Israeli cyber firms had been trained in Unit 8200 or related units. Unit 8200 has long been associated with aggressive and intrusive surveillance of Palestinians, including through "the collection of embarrassing sexual, financial or other information". Cyber-security startups established by former members of these units have tested their technologies with lucrative contracts from the Israeli military before bringing the products to the international market. For example, tech startup AnyVision (now called Oosto) developed an extensive facial recognition network across the West Bank for the Israeli army, a model that one *Haaretz* journalist described as "competing with the Chinese regime" in its intrusiveness. "These surveillance products are often marketed and sold as 'field tested'," says Marwa Fataftah of Access Now.[3] In 2021 AnyVision secured $235m in an investment round led by SoftBank's Vision Fund 2. SoftBank's technology portfolio, which invests in "global AI innovators", has been heavily backed by Saudi Arabia's Public Investment Fund.

The development of Israel's cyber-security industry has played a central role in the Israeli state's deepening strategic links with the UAE, Saudi Arabia, and Bahrain – a process that culminated in Israel signing the Abraham Accords with UAE, Bahrain, and Morocco in 2020.

Recent years have seen the emergence of a raft of joint UAE-Israel technology projects. These include a joint "innovation office" to provide the UAE with access to Israel's "most innovative and cutting edge technologies", including cyber-security; 'smart cities' and drone technologies; an artificial intelligence (AI) research and development hub in Abu Dhabi; and a UAE-Israeli tech investment fund of $100m. Meanwhile, Saudi Arabia has hosted Israeli tech entrepreneurs to pursue investments in Israeli companies and funds, with the expectation that these firms would play a major role in the planned NEOM smart city, the site of the first meeting between Israeli and Saudi leaders in late 2020.

Some Israeli activists argue that these relationships have been forged through "Pegasus diplomacy", whereby the Israeli government approves the export of NSO technology to Gulf states in return for the normalisation of their relationships with Israel. The UAE bought two separate licences to operate Pegasus, one each for Abu Dhabi and Dubai. The emirate's ruler allegedly used the latter to hack into the phone of his estranged wife amid a divorce battle in the London courts. The former has allegedly been used to access 10 Downing Street's communications system.

In 2019, seeking Riyadh's tacit support for normalisation and access to Saudi airspace for Israeli airlines, then prime minister Benjamin Netanyahu personally approved the renewal of NSO Group's licence to export Pegasus to Saudi Arabia, turning a blind eye to the role the software had played in the country's crackdown on human rights activists (perhaps including Khashoggi).

Cellebrite, an Israeli cyber-security firm owned by Sun Corporation – which has marketed its products to the Belarusian and Hong Kong authorities – helped Saudi Arabia hack into a phone held by the Saudi Justice Ministry in 2020. In 2021 Citizen Lab found evidence suggesting that hacking software provided by Israeli firm Candiru – which the US has since placed on an export control list alongside NSO Group for activities that "threaten the rules-based international order" – has been operated by UAE and Saudi Arabia.

Social control: Mass surveillance and the Chinese model

Authoritarian governments in the Middle East increasingly engage in comprehensive surveillance based on the Chinese model, using AI-led programmes that analyse massive quantities of personal data to "identify threats, trends and opportunities for state action", as a recent Project on Middle East Political Science study on digital authoritarianism puts it. Dubbed "dataveillance" as early as the 1980s, such a strategy may be out of reach for poor, low-capacity Arab states. But this is not the case for wealthier countries in the region. The founding board of NEOM once declared that the project "should be an automated city where we can watch everything … where a computer can notify crimes without having to report them or where all citizens can be tracked." The state may portray such capabilities as a means to enhance service delivery and efficiency, but there is a substantial risk that they will facilitate human rights violations.

When citizens are aware they are subject to pervasive monitoring and data collection, this can lead them to accept the status quo and limit their efforts to imagine alternative social and political realities. Such a chilling effect can alter the behaviour of individuals who are politically engaged but seek to avoid negative consequences in other areas of their lives. Dubai has mooted a behavioural reward system that seems to draw inspiration from the Chinese social credit system. As Jones notes, there is an alignment between the interests of tech companies that collect personal data as part of a business model sometimes termed "surveillance capitalism" and the interests of authoritarians who collect personal data for the purposes of social control.[4]

The covid-19 pandemic provided governments around the world with a reason to massively increase their collection of citizens' personal data, often with the introduction of compulsory, highly intrusive apps that monitor their movements. The government in Bahrain threatened to severely punish individuals who failed to use its covid-19 app – which captured location data through GPS and uploaded it to a central database, tracking the movements of users in real-time – or wear the electronic wristband that came with it. Kuwait's covid-19 app uploaded users' location data to a central server every ten minutes. The UAE used thermal cameras in airports and malls, and on police officers' helmets, to track the temperature of passers-by. Just as governments around the world used the security crisis of 9/11 to permanently adopt a raft of restrictive laws and measures, they seem likely to retain many data surveillance practices introduced in response to covid-19.

Governments' collection and use of biometric information are particularly concerning. The Israeli authorities have reportedly collected the images of at least 450,000 Palestinians with live facial recognition (LFR) software that, according to its manufacturer, uses CCTV feeds to "identify individuals and objects … and then track targets as they move between different feeds". Around 95 per cent of East Jerusalem is covered by CCTV. This has a profound psychological effect on people who know they are almost always being filmed. One man told the Washington Post that, when his six-year-old daughter dropped a teaspoon from the family's roof, soldiers came to his home to tell him that he would be cited for throwing stones. Israeli soldiers are incentivised to take as many photos as possible of Palestinians, including children, so they can be matched to live video footage.

In 2021, following pressure from NGOs, the European Parliament called for a permanent ban on the automated recognition of individuals in public spaces. The Council of Europe has also raised the alarm about LFR in public spaces due to "the intrusiveness it bares (sic) upon the right to privacy and the dignity of individuals, coupled with a risk of adverse impact on other human rights and fundamental freedoms". Systems that include emotion recognition software – which are most common in China – are particularly alarming.

Gulf states are eagerly adopting facial recognition technologies. In March 2020, Abu Dhabi police upgraded their patrol cars with a live biometric facial recognition system. Dubai's Oyoon security system uses the network of 300,000 cameras across the city to analyse data and "detect suspects". NTechLab, which is partly owned by the Russian government, and which helps to operate Russia's vast biometric surveillance system, opened an Abu Dhabi office in 2021 and won the contract to carry out video monitoring of Expo 2020. The company claims that its products can identify people's emotions. One of its tools is designed to classify faces based on their perceived ethnicity or race. In Gulf countries such as Qatar – where racial discrimination is a major concern and people from ethnic minorities at heightened risk of harassment by state authorities – migrant workers may now be flagged as a security risk if LFR technologies detect that they have visited a specific public space multiple times.

The UAE has pioneered the use of predictive policing – in which historical data inform future strategies and resource allocation – in the Gulf, with Dubai's police force announcing in 2016 its intent to use this approach and, more recently, developing an AI platform to guide decision-making. Bahrain has reportedly been using PredPol software to anticipate protests.

In Europe and North America, predictive policing has been shown to reinforce discriminatory policing practices, and to have a particularly significant impact on racial or other minorities. Multiple studies show how data-driven or algorithmic decision-making tends to result in discrimination against already marginalised or excluded communities. This is because predictive policing depends on so-called dirty data – inaccurate, skewed, or systemically biased data that has been generated using patterns of behaviour shaped by political, social, and other biases. Some scholars now go further, arguing that racial inequality is in fact "a feature, not a bug of data capitalism". In authoritarian countries, there is a heightened risk that the authorities will abuse these types of systems. And, as one European Parliament study points out, AI-driven data-collection systems affect "wider and harder to delineate categories of victims" than other forms of digital authoritarianism – which makes them more difficult to challenge and, accordingly, more likely to be accepted by the population.

While Gulf and other Arab states are traditional allies of the US, their deepening commercial and political relationships with China provide them with a mass-surveillance model and partner – one that will sell them technological capabilities at a relatively low price. China has used the Digital Silk Road, the technological component of its Belt and Road Initiative, to sign memorandums of understanding with Egypt, Saudi Arabia, and the UAE. These agreements pave the way for intensified technology transfer, training programmes, and investments in infrastructure by Chinese tech firms. In this way, China will become increasingly important to Arab technology stacks – the layers of a digital communications ecosystem.

China and the UAE concluded in 2018 a comprehensive strategic partnership that covers work on AI. Chinese AI firm Sense Time – which the US sanctioned in 2021 for its involvement in facial recognition technology that can reportedly identify ethnic Uighurs even when they have beards or are wearing hats or sunglasses – established in 2019 a research and development hub in Abu Dhabi. Group 42 – the Abu Dhabi-based company behind ToTok – partnered with Sinopharm in 2021 to produce a covid-19 vaccine. Huawei is now helping Saudi Arabia launch its National AI Capability Development Program.

Huawei has made substantial inroads into the Gulf markets for 5G and cloud services. Saudi Arabia has chosen to use Huawei's 5G technology in NEOM despite the objections of the US – which has concerns about the firm's relationship with the Chinese Communist Party, as well as the risk that Chinese 5G wireless technology will serve as a platform for cyber-attacks and influence operations. Israel has made more efforts than the UAE or Saudi Arabia to manage US concerns over Huawei, apparently reasoning that its security relationship with Washington is more important than its commercial relationship with China. In 2019 Israel established a committee to screen foreign investments with security implications, which was implicitly focused on China. Washington's aggressive posture on Huawei is explicitly rooted in security and strategic concerns. But there are good reasons to be concerned about the company's record on human rights, given its involvement in smart policing in Xinjiang province and its promotion of ToTok.

More broadly, China is an apparently successful model of digital authoritarianism. One Saudi official told the *Financial Times* in 2021 that "there's a lot to learn from China and its ability to develop the way it has is predicated on the fact it's not a democracy." Watching these developments with concern, the US has formed initiatives such as the Freedom Online Coalition, a group of 34 states "committed to protecting and promoting online freedoms domestically and abroad". The fierce competition between the US and China over technology undermines efforts to develop a unified global vision of digital governance. Control of internet standards and protocols is a critical part of this contest: China and Russia argue that governments should have more control of the internet through the International Telecommunication Union (ITU), while the US and its allies prefer a bottom-up approach led by technologists – which Beijing and others see as giving excessive power to American technology corporations. China has pushed for the ITU – rather than alternative, multi-stakeholder, and typically Western-led forums – to lead on the international standardisation of AI.

China uses financing under the Digital Silk Road to promote its technology standards. Authoritarian states increasingly apply these standards, which are unlikely to involve concepts such as "privacy by design

”, an approach to systems development that requires data protection to be taken into account throughout the process.

Europe's response to digital authoritarianism

The global technological landscape is dominated by a small number of tech companies that are accountable primarily to their shareholders and act as what one European Parliament report calls the “ gatekeepers of fundamental rights”. This is a challenging environment for the EU, which also remains digitally dependent on both the US and China in areas ranging from chat platforms to telecommunications equipment – to the extent that some European officials speak of the risk that their countries will become “cybercolonies”. Europe is not home to any of the dominant tech platforms; nor does it produce hardware on a significant scale. As a result, Europe is sometimes caught between the two powers as they compete for technological and industrial dominance. For example, in 2020, European governments came under intense pressure from both Washington and Beijing over the use of Huawei in European 5G networks.

In this contested space that leaves little room for multilateralism, European policymakers have sought to lead the way through unilateral digital regulation. They have adopted a markedly different approach from the US, whose efforts to address the impact of online harms have been held back by both partisan rivalries and a desire to encourage innovation in the private sector. Accordingly, Washington’s efforts in the area have been limited to tackling “specific narrow issues that tend to be of primary concern to US citizens, such as antitrust laws, addressing misinformation online, and data privacy” – as Tamara Kharroub of the Arab Center DC puts it.[5]

The EU’s Digital Services and Markets Acts (DSA and DMA) will provide a clear set of rules for digital platforms. The DSA is designed to create safer online spaces by requiring social media platforms to assess and manage systemic risks posed by their services. Its provisions apply to large platforms, hosting services, and intermediary services. Among other things, the act will make it possible to challenge content-moderation decisions, will require transparency measures on algorithms used for recommendations, and will obligate large platforms and search engines to prevent the misuse of their systems by taking risk-based action and engaging in independent audits of their risk management systems. Human rights groups have welcomed the act as a meaningful effort to check the power of technology companies and protect individuals.

This is an example of the EU using regulations and the power of its market to encourage other powers to follow European practices. The union’s aims in this area have been clear in relation to, for instance, Elon Musk’s plan to take over Twitter. The EU internal market commissioner responded to news of the proposed deal with a stark public warning that: “any company operating in Europe needs to comply with our rules – regardless of their shareholding. Mr Musk knows this well.”

The EU’s forthcoming legislation that requires large firms to carry out human rights due diligence could also have an impact on tech regulation. This legislation would have extraterritorial reach – which is crucial to addressing the transnational effects of digital technologies. For example, the regulation would obligate companies planning to engage with customers in high-risk contexts to ask themselves difficult questions at the point of market entry – a process that might have discouraged Nokia from extensively supporting the development of Russia’s vast SORM state surveillance system. However, the legislation will only apply to companies with more than 500 staff and a net turnover of at least €150m. This means that it will not have an impact on small and medium-sized enterprises, including those such as European public relations firms that run influence campaigns for authoritarian regimes.

As part of its push on technology regulation, the European Commission published a draft Artificial Intelligence Act in 2021, seeking to set global standards for trustworthy and ethical AI. This reflects a concern that, as Ulrike Franke and José Ignacio Torreblanca argue, “if the EU does not act, others will impose their AI standards … Should they develop and promote these rules sufficiently, the EU would be reduced to following standards that it could not influence.” The draft act proposes a framework that prohibits a small number of uses of AI, such as for China’s social credit scores, and categorises others, such as biometric and border security, as “high risk” and requiring greater monitoring and scrutiny. Civil society groups welcome the overall thrust of the proposal but have criticised its proposed risk ratings as inflexible; called for the act to place more responsibility on those who buy and deploy systems as well as those who develop them; and recommended that it introduce mechanisms through which individuals affected by AI systems can claim a remedy for harms suffered. The draft proposal the European Parliament published in April 2022 added a prohibition on the development or use of AI for predictive policing, arguing for a more cautious approach to a whole swathe of other technologies, such as deep-fake software and systems designed for elections and healthcare triage. A report by the Brookings Institution suggests that while the act will have the Brussels effect – in which the EU’s regulations have a transformative impact beyond Europe, driving others to meet its standards to gain access to European markets – it may be fragmented and not as strong as European leaders claim.

As Manuel Langendorf argues, one way the EU can engage with governments in the Middle East is to help them construct policy frameworks and laws that promote the digital economy while respecting individual rights to privacy and free expression. This would have, as he puts it, “the benefits of a policy framework and a set of regulations that guarantee the free flow of information and support the internet's role in socio-economic development." Data protection is one area of engagement: the EU's 2018 General Data Protection Regulation (GDPR) could provide a model for governments in the region. And European technology firms could gain a firmer footing in the Middle East, as they seek to establish a physical presence in countries in the region and capitalise on the digital transformation – and data localisation – pursued by countries such as Saudi Arabia, Egypt, Jordan, and the UAE as part of their diversification programmes.

However, there are limits to such laws in authoritarian countries, even when they appear to broadly align with European standards. The Egyptian subsidiary of French company Orange is constructing a data centre that will host all the smart-city platforms of Egypt's new administrative capital, east of Cairo, while UK telecoms firm Vodafone has been in talks about support for the city's 5G networks. Egypt has put in place a data protection law that, in many respects, complies with international standards and draws on the GDPR. The law strictly prohibits access to – and collection, processing, transfer, and retention of – sensitive personal information, such as biometric data, unless there is explicit written consent from the user and it is licenced by the data regulator. However, the flaws in the legislation are so fundamental that Access Now has suggested that its primary goal is data control rather than protection: the national security services – many of which will operate out of the new administrative capital – are exempt from the law and will sit on the board of the data regulator, while tech companies are obliged to keep personal data for 180 days and to allow the authorities to access it.

Similarly, Jordan's proposed new data protection agency would include members of the security agencies, effectively rendering it toothless on the most critical data protection questions in the country.

In Saudi Arabia, Google has moved to set up a cloud region in partnership with Aramco. SMEX points out that Google services in the country will be placed under the authority of the Saudi Communications and Information Technology Commission, which can direct the firm to remove or block content that may fall foul of Saudi Arabia's repressive 2007 cyber-crime legislation. Google claims to have carried out a human rights impact assessment of the controversial project, which it says is "of limited scope". In June 2022, more than half of the company's independent shareholders voted for a resolution that asked the company to "commission a report assessing the siting of Google cloud data centers in countries of significant human rights concern". But this was overruled by executives at the firm. Project Nimbus, a massive cloud computing project in Israel involving Google and Amazon, has generated similar concerns among shareholders and the companies' employees.

The EU has long benefited from the Brussels effect. The union uses its adequacy framework to attempt to influence data protection rules, and incentivise better practices, in other jurisdictions. For data sharing purposes, the EU treats countries it assesses as having adequate data protection rules as if they were members of the bloc, allowing information to flow freely between them.

Several states in the Middle East have recently introduced new data protection laws, possibly with half an eye on the EU's requirements. But, so far, only Israel has met these requirements (in 2011, prior to the adoption of the GDPR in 2018). As this does not apply to the West Bank, the Golan Heights, East Jerusalem, or the Gaza strip, it excludes the mass surveillance of Palestinians under Israeli occupation from the EU's decision-making. With the union now reviewing Israel's adequacy status, it is unclear whether Israeli tech firms' involvement in the hacking of European politicians, officials, and private citizens will affect the country's status.

The EU's attempts to regulate the export of high-risk surveillance technologies have been complex and divisive. The European Commission and the European Parliament have pushed for tougher controls on exports of technologies that can be used for both civilian and military purposes, with support from member states such as Germany and the Netherlands. In this, they have faced resistance from member states that have financial interests in the technology sector. European technology firms have argued against changes that affect the EU's competitiveness through what they see as unnecessary and disproportionate restrictions on the transfer of benign technologies. Member states such as Sweden, France, Italy, Ireland, Cyprus, and Finland pushed back against a 2016 Commission proposal to tighten the human rights requirements in 2009 regulations on dual-use technology. They contend that tighter requirements would not only have commercial disadvantages but would also damage security relations with key strategic partners. This could affect, for example, France's sale of surveillance equipment to Egypt – which the Commission has scrutinised.

It was not until 2021 that the EU agreed on an updated regulation that required member states to "consider the risk" of dual-use products' involvement in human rights abuses – a weaker standard than the union has adopted on military equipment and technology, for which states must deny export licences if there are such risks. The updated dual-use regulation establishes a new "catch-all control" under which member states can decide to subject new items to export control measures if they identify a potential human rights risk. In this way, the new regulation has created a mechanism for establishing an EU list of controlled cyber-surveillance items, reducing the union's reliance on somewhat problematic international regimes such as the Wassenaar Agreement.

The new requirements are limited to dual-use items that enable surveillance by "monitoring, extracting, collecting or analysing data from information and telecommunication systems" – a definition that some civil society groups fear will be narrowly interpreted to exclude biometric and facial recognition technologies, for example. The regulation anticipates that other emerging technologies – such as AI – will likely create security and human rights concerns, providing a mechanism through which states could place export controls on them. The Stockholm International Peace Research Institute concludes that “the expanded mechanism to control unlisted items potentially sets the stage for an uneasy relationship between those pushing for more autonomous EU controls – namely, the [European Parliament] and the Commission – and those with the power to determine whether and how the controls are used – that is, the member states.”

However, there are real questions about whether risk-based regulation is an adequate response to the dangers associated with surveillance technologies such as Pegasus. This has led UN human rights experts to call for a global moratorium on the sale and transfer of such technologies until states can effectively control them. The EU data supervisor called for a ban on the development or deployment of any technologies with these capacities within the EU, recognising the “paradigm shift” they represented and their threat to democratic values. Short of this, his report called for far greater democratic and judicial oversight of the regulation of these technologies. Proponents of a moratorium or a ban argue that Pegasus-style technology should be treated as an inherently harmful weapon along the lines of cluster munitions. Meanwhile, critics of these measures suggest that surveillance technology is relatively inexpensive to purchase and transfer – meaning that, under a ban, there would be a flourishing black market for it that would cede control to the worst actors.

The EU attempts to address the risk of digital authoritarianism in various ways beyond market regulation and the Brussels effect. In the multilateral sphere, the EU and its member states have been increasingly active in efforts to ensure that the UN framework adapts to emerging technologies, including through UNESCO’s work on AI. In 2021, the EU helped block a proposal at the ITU for a standard on facial recognition that would have allowed for the processing of biometric personal data without data protection or privacy safeguards. In recent weeks, the EU has endorsed the Biden administration’s Declaration on the Future of the Internet, an initiative primarily aimed at reinforcing democracy in European and other countries where it is faltering rather than at achieving a global consensus.

The European Council’s 2014 guidelines on freedom of expression commit the EU to “work against any attempts to block, jam, filter, censor or close down communication networks or any kind of other interference that is in violation of international law.” The union can play a positive role in this area: in 2017 it supported Palestinian civil society groups’ calls for the Palestinian Authority to withdraw clauses in its cyber-crimes law targeting political expression and political activism, resulting in amendments to the law the following year.[6]

However, the EU has underperformed on this elsewhere in the Middle East. The European External

Action Service's human rights report for 2021, the year in which the Pegasus revelations emerged, says only that the EU "used some of its political dialogues, including human rights dialogues, to raise concerns about spread of internet shutdowns, online censorship and mass and targeted arbitrary surveillance" without specifying the countries in question. Human rights and political dialogues generally take place in private. A European Parliament report on digital authoritarianism argues that the union "has not been willing to incur significant costs, in terms of letting trends in digital repression impact its commercial and strategic interests".

In line with the recent increase in malicious behaviour in the digital space, the EU has also introduced a sanctions regime targeting individuals responsible for cyber-attacks on the union, its member states, third countries, or international organisations. It imposed these sanctions for the first time in 2020, targeting Chinese, Russian, and North Korean entities – some of which had carried out an attack on the Organisation for the Prohibition of Chemical Weapons. But the EU has not yet used such sanctions in response to human rights violations. Nor has it used its global human rights sanctions regime, adopted in 2020, in relation to digital repression.

Nonetheless, the EU can play a crucial role in supporting human rights defenders and activists who are victims of digital repression or seek to combat it. The union's human rights defenders mechanism provides training in digital security, disbursing 47 emergency grants for digital security and protection measures in 2021. The mechanism is designed to address threats such as attacks on human rights defenders' communications, theft or misuse of their personal and professional information, a lack of adequate security equipment, and online surveillance. Meanwhile, the European Endowment for Democracy provides important backing to activists and citizen journalists by working to create a safer online environment. For example, the endowment has supported independent online news platform *Beirut Today*, which operates in a polarised political climate, and the Verify-Sy fact-checking service, which has debunked thousands of fake news stories about the conflict in Syria.

However, the EU has undermined its own credibility in countering digital authoritarianism with its migration policies, which have led it to provide surveillance equipment and training to security agencies in the Balkans and Africa as part of an effort to externalise its border controls. It is unclear how the EU considered human rights risks in this process. For example, the union provided the government of Niger with a simulator of a mobile-phone tower to intercept communications, even though the country has no laws that regulate such intrusive equipment. The European ombudsman announced in late 2021 that it was opening an investigation into the provision of the equipment and related human rights assessments.

European policy priorities

European policymakers need to prioritise their response to the threat of spyware, which human rights experts argue can cause the kind of harms often associated with conventional weapons. Decisive action on spyware would not only support human rights activists around the world but also serve the EU's security interests, given that the communications of European officials have been intercepted using this technology. In this, policymakers should study the European data protection supervisor's recommendations: while the prospect of a full prohibition on spyware might be unpalatable to member states, it is hard to overstate the gravity of the threat it poses to privacy, freedom of expression, and – ultimately – democratic systems. At a minimum, the EU should dramatically increase democratic and judicial oversight of the development of, and trade in, surveillance equipment.

In the meantime, European policymakers should look to impose costs on those involved in the trade of such tools that are used to violate human rights – a task complicated by the fact that some European law enforcement and intelligence agencies have employed Pegasus. The EU's lack of direct action against NSO Group since the Pegasus revelations is striking. Indeed, in June 2022, just as the European Parliament was preparing for a hearing into the activities of NSO Group, the company was sponsoring an event in Prague. The lack of consequences for NSO Group could contribute to a sense of impunity among spyware firms. The union's review of Israel's adequacy status will signal how it intends to apply its commitment to data protection to a strategic partner that has been at the centre of a privacy breach with global ramifications.

More broadly, the EU should raise the profile of spyware-related human rights violations in bilateral discussions with partners such as the UAE, Egypt, Saudi Arabia, and Qatar. It is still unclear whether the union mentioned digital repression in its first human rights dialogue with Saudi Arabia in late 2021.

The EU should also review its policy of providing surveillance equipment to its migration partners to support its goals of reducing migration flows. This practice not only has the potential to facilitate human rights violations but also damages the union's credibility on digital authoritarianism.

The lesson of the scandal around NSO Group – which may have received export licences in Europe through subsidiaries as well as in Israel – is that Europeans need to pay far greater attention to the private sector's role in providing technologies to third countries. Alongside its suite of digital regulations, the EU should provide specific guidance on how its human rights due diligence regulation applies to the technology sector – including by setting expectations for companies' approach to risk mitigation when they provide technologies or digital services that are likely to be used by government agencies. Meanwhile, member states that provide diplomatic, advisory, or financial support to domestic tech firms should carry out risk assessments on products and services they support that could be used for digital repression.

The EU has taken a leading role in the regulation of AI and is seeking workable international governance arrangements for this enabling technology – potentially in the form of a legally binding treaty through the Council of Europe. A treaty could potentially include a requirement for "Human Rights, Democracy, and the Rule of Law Impact Assessments" for certain systems – which would be a significant development. The union's normative approach should provide an important complement to the United States' more geopolitical efforts in the area. The EU should now make a case for international controls on AI by stressing the potential ramifications of the poor regulation of the technology on economic, social, and cultural rights – not least the risks of discrimination, marginalisation, and exclusion to specific communities. Arguably, one of the challenges in broadening the global coalition around the protection of digital rights has been the tendency to focus on the implications for individuals of privacy and data breaches rather than the impact on communities.

Finally, the resources the EU allocates to initiatives to defend against digital authoritarianism still pale in comparison to the scale of the challenge, with civil society groups in many Middle Eastern countries almost entirely unable to communicate domestically or internationally using the internet. In this context, it is more urgent than ever for the EU take up a 2015 European Parliament resolution calling for a human rights and technology fund to support such activists.

Acknowledgements

The author would like to thank all the experts he consulted for this paper, as well as Rasha Abdul Rahim, Phil Dawson, and Joe Westby for their advice. He would also like to thank Hugh Lovatt and Chris Raggett of ECFR for their support with reviewing and editing the paper.

About the author

James Lynch is a visiting fellow at ECFR and a founding co-director of FairSquare, a human rights research and advocacy group. He worked at Amnesty International from 2011 to 2017 – where he was, among other roles, deputy director of the Middle East and North Africa programme, and where he was targeted by a fake NGO of unknown provenance claiming to work on human rights and the Qatar World Cup. Lynch worked for the UK Foreign and Commonwealth Office between 2004 and 2011, mainly focusing on the Middle East.

[1] Online event hosted by the Council for Arab-British Understanding, 26 April 2022.

[2] Remote interview with Marc Owen Jones, 10 June 2022.

[3] Remote interview with Marwa Fataftah, 10 May 2022.

[4] Online event hosted by the Council for Arab-British Understanding, 26 April 2022.

[5] Email correspondence with Tamara Kharroub, 21 June 2022.

[6] ECFR researcher’s discussion with a European official, Jerusalem, September 2018.

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Lykke Friis, and Norbert Röttgen.

- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.

- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and "friends of ECFR" gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions. ecfr.eu

The European Council on Foreign Relations does not take collective positions. This paper, like all publications of the European Council on Foreign Relations, represents only the views of its authors. ISBN: 978-1-914572-56-2. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA, United Kingdom.