Pegasus and the EU’s external relations
Abstract
This study - commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs at the request of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA) – analyses the proliferation of new and emerging technologies used for repression and social control. While these technologies still have the potential to positively enhance democratic values and human rights, repressive regimes actively deploy these tools for their own strategic advantage. In particular, the proliferation of commercial spyware, such as Pegasus software, is a big concern. The EU should place a much higher priority in countering government use of these tools.
This document was requested by the European Parliament's Committee of Inquiry to investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA).

AUTHORS OF THE STUDY
Authors of the Pegasus update: Steven FELDSTEIN, Senior Fellow, Carnegie Europe, Brussels and Richard YOUNGS, Senior Fellow, Carnegie Europe, Brussels & Professor of International Relations, University of Warwick, UK.
Authors of the original study: Dorota GŁOWACKA, Panoptykon Foundation, Poland and Richard YOUNGS, Senior Fellow, Carnegie Europe, Brussels & Professor of International Relations, University of Warwick, UK.
Coordination: Joanna SMĘTEK, Ecorys, Poland and Katarzyna LUBIANIEC, Ecorys, Poland

ADMINISTRATORS RESPONSIBLE
Mariusz MACIEJEWSKI
Ottavio MARZOCCHI

EDITORIAL ASSISTANT
Ivona KLECAN

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens’ Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in January 2023
© European Union, 2023

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT
The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.
Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.
© Cover image used under licence from Adobe Stock.com
CONTENTS

LIST OF ABBREVIATIONS 6
LIST OF BOXES 10
LIST OF FIGURES 10
LIST OF TABLES 10
EXECUTIVE SUMMARY 11

1. INTRODUCTION 18
  1.1. Objectives and scope of the study 18
  1.2. Definitions of key concepts 20
  1.3. Note on methodology 23

2. TRENDS IN THE USE OF DIGITAL TECHNOLOGIES FOR REPRESSION AND SOCIAL CONTROL 25
  2.1. Expansion of widespread biometric surveillance and algorithmic decision-making 25
  2.2. Emergence of public health surveillance systems 29
  2.3. Digital tools of information control 31
  2.4. Next generation repression toolkit 38
  2.5. Transnational dimensions of digital repression 41
  2.6. Pegasus and equivalent surveillance spyware 44
    2.6.1. The emergence of targeted surveillance and its models of operation 44
    2.6.2. Commercial spyware surveillance chain 45
    2.6.3. Global proliferation of commercial spyware 46
    2.6.4. Emergence of Cytrox Predator 48
    2.6.5. Cellebrite’s data extraction technology 49
    2.6.6. Europe as a “nexus” for commercial spyware 50
    2.6.7. Policy discussion around Pegasus and equivalent surveillance spyware 53
  2.7. Conclusions 54

3. OVERVIEW OF THE INTERNATIONAL HUMAN RIGHTS FRAMEWORK 57
  3.1. Introduction 57
  3.2. AI and algorithmic decision-making systems 60
  3.3. Surveillance in a digital age 65
  3.4. Disruptions to free flow of information online 69
  3.5. Human rights and private actors 73
  3.6. Conclusions 76
4. **THE EU’S DEMOCRACY AND HUMAN RIGHTS TOOLBOX**

4.1. General evolution of the EU toolbox
   
   4.1.1. Evolution of the core toolbox
   
   4.1.2. Digital elements in the policy framework
   
   4.1.3. EU Human Rights Guidelines for Freedom of Expression Online and Offline
   
   4.1.4. Other instruments and initiatives

4.2. Restrictive measures and conditionality
   
   4.2.1. Democracy and Human Rights Sanctions
   
   4.2.2. Cyber sanctions
   
   4.2.3. Conditionality
   
   4.2.4. Restrictions on surveillance equipment

4.3. Dialogues and multilateral engagement
   
   4.3.1. Human rights dialogues
   
   4.3.2. Multilateral dialogue and engagement
   
   4.3.3. Engaging the private sector

4.4. Funding
   
   4.4.1. European Instrument for Democracy and Human Rights
   
   4.4.2. Media pluralism
   
   4.4.3. Civil society and digital activism
   
   4.4.4. Protecting activists from repression
   
   4.4.5. European Endowment for Democracy

4.5. Overlaps with cyber-security and influence operations
   
   4.5.1. Stratcom
   
   4.5.2. Cyber funding

4.6. Possible responses to Pegasus and equivalent surveillance spyware
   
   4.6.1. How has the EU toolbox dealt with spyware?
   
   4.6.2. Sanctions
   
   4.6.3. Regulating trade in spyware
   
   4.6.4. The Wassenaar Arrangement
   
   4.6.5. Diplomatic relations
   
   4.6.6. Funding

4.7. EP instruments and contributions

4.8. Conclusions - assessment of the toolbox’s evolution

5. **CONCLUSIONS AND RECOMMENDATIONS**

5.1. Conclusions and recommendations in relation to the initial study

5.2. Conclusions and recommendations in relation to Pegasus and equivalent surveillance spyware
## REFERENCES

- Primary Sources
- Secondary Sources – books and articles
- Joint/ Group Publications
- List of consulted stakeholders

## ANNEXES

- Interview topic guide – EU institutions
- Interview topic guide – CSOs and other respondents
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
<td>Second Generation Cellular Network</td>
</tr>
<tr>
<td>AChHPR</td>
<td>African Charter on Human and Peoples’ Rights</td>
</tr>
<tr>
<td>ACHPR</td>
<td>African Commission on Human Rights</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>AU</td>
<td>African Union</td>
</tr>
<tr>
<td>B-Tech</td>
<td>Business and Human Rights in Technology Project</td>
</tr>
<tr>
<td>BSI</td>
<td>Bureau of Special Investigations (Myanmar)</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CEPEJ</td>
<td>European Commission for the Efficiency of Justice</td>
</tr>
<tr>
<td>CESCER</td>
<td>Committee on Economic, Social and Cultural Rights</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>COMPAS</td>
<td>Correctional Offender Management Profiling for Alternative Sanctions</td>
</tr>
<tr>
<td>COVID-19</td>
<td>Coronavirus disease 2019</td>
</tr>
<tr>
<td>CSO</td>
<td>Civil Society Organization</td>
</tr>
<tr>
<td>CT</td>
<td>Counter Terrorism</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DMA</td>
<td>Digital Market Act</td>
</tr>
<tr>
<td>DNA</td>
<td>Deoxyribonucleic Acid</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DROI</td>
<td>Subcommittee on Human Rights</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Services Act</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention of Human Rights</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>ECOWAS</td>
<td>Community Court of Justice of the Economic Community for West African States</td>
</tr>
<tr>
<td>ECRI</td>
<td>European Commission on Racism and Intolerance</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDAP</td>
<td>European Democracy Action Plan</td>
</tr>
<tr>
<td>EEAS</td>
<td>European External Action Service</td>
</tr>
<tr>
<td>EED</td>
<td>European Endowment for Democracy</td>
</tr>
<tr>
<td>EFM</td>
<td>Electoral Follow-up Mission</td>
</tr>
<tr>
<td>EIDHR</td>
<td>European Instrument for Democracy and Human Rights</td>
</tr>
<tr>
<td>ENISA</td>
<td>EU Agency for Network Information Security</td>
</tr>
<tr>
<td>EOM</td>
<td>Election Observation Mission</td>
</tr>
<tr>
<td>EP</td>
<td>European Parliament</td>
</tr>
<tr>
<td>ESC</td>
<td>European Social Charter</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FOC</td>
<td>Freedom Online Coalition</td>
</tr>
<tr>
<td>FRA</td>
<td>EU Agency for Fundamental Right</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographical Information Systems</td>
</tr>
<tr>
<td>GNI</td>
<td>Global Network Initiative</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HLPDC</td>
<td>High-level Panel on Digital Cooperation</td>
</tr>
<tr>
<td>HRD</td>
<td>Human Rights Defenders</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>IACHR</td>
<td>Inter-American Commission on Human Rights</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICESCR</td>
<td>International Covenant on Economic Social and Cultural Rights</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IGF</td>
<td>Internet Governance Forum</td>
</tr>
<tr>
<td>iOS</td>
<td>iPhone Operating System</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IXP</td>
<td>Internet Exchange Point</td>
</tr>
<tr>
<td>MENA</td>
<td>Middle East and North Africa</td>
</tr>
<tr>
<td>MEP</td>
<td>Member of the European Parliament</td>
</tr>
<tr>
<td>MFF</td>
<td>Multiannual Financial Framework</td>
</tr>
<tr>
<td>NDICI</td>
<td>Neighbourhood, Development, and International Cooperation Instrument</td>
</tr>
<tr>
<td>NetzDG</td>
<td>Germany Network Enforcement Law</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-governmental organization</td>
</tr>
<tr>
<td>OAS</td>
<td>Organization of American States</td>
</tr>
<tr>
<td>OHCHR</td>
<td>Office of the United Nations High Commissioner for Human Rights</td>
</tr>
<tr>
<td>OIC</td>
<td>Organization of the Islamic Conference</td>
</tr>
<tr>
<td>OSCE</td>
<td>Organisation for Security and Co-operation in Europe</td>
</tr>
<tr>
<td>PACE</td>
<td>Parliamentary Assembly</td>
</tr>
<tr>
<td>PESCO</td>
<td>Permanent Structured Cooperation</td>
</tr>
<tr>
<td>RAB</td>
<td>Rapid Action Battalion</td>
</tr>
<tr>
<td>RAT</td>
<td>Remote Access Trojans</td>
</tr>
<tr>
<td>SEC</td>
<td>Security Exchange Commission</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>T-PD</td>
<td>Consultative Committee</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>UFED</td>
<td>Universal Forensic Extraction Device</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNESCO</td>
<td>United Nations Educational, Scientific and Cultural Organization</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Networks</td>
</tr>
<tr>
<td>WHO</td>
<td>World Health Organization</td>
</tr>
</tbody>
</table>
LIST OF BOXES
Box 1: Examples of algorithmic harm 29
Box 2: Implications of internet shutdowns in the COVID-19 era 33
Box 3: Cyber sovereignty in China and Russia 37
Box 4: Digital dominance of the largest online platforms in numbers 40
Box 5: Use of Pegasus in Thailand 47
Box 6: Global spread of spyware – updated indicators 52
Box 7: Main human rights international treaties and rights most affected by the use of digital technologies for repression and social control 58
Box 8: International human rights mechanisms undermined 64
Box 9: Three pillars of the ‘Protect, Respect and Remedy’ Framework 74
Box 10: Civil society and multistakeholder initiatives on business & human rights in a digital space 75
Box 11: EU toolbox on the ground: Myanmar 95
Box 12: EU toolbox on the ground: Kyrgyzstan 97
Box 13: EU relations with Israel in the light of Pegasus case 104

LIST OF FIGURES
Figure 1: Number of documented internet shutdowns across the world between 2015 and 2019 33
Figure 2: Global spread of commercial spyware and digital forensics, 2011-2022 53

LIST OF TABLES
Table 1: Examples of human rights implications of mandatory pandemic-related apps 30
Table 2: Examples of new laws challenging internet freedom 35
EXECUTIVE SUMMARY

Study objectives and scope

This study is an update of the 2021 study on digital technologies as a means of repression and social control prepared at the request of the European Parliament’s DG EXPO. In terms of scope, the update focuses on any situation related to the use of Pegasus-type spyware that has a foreign element (notably because the spyware is produced in a non-EU country, or because it is used by a non-EU country, or because it targets non-EU citizens).

The objectives of the update were to:

- describe the most important and sufficiently documented cases of alleged or confirmed use of Pegasus and of similar spyware with foreign element at global;
- examine the international, European and EU legal and policy framework on human rights (including privacy and data protection), its relevance and applicability to the production, trade and use of spyware in the various abovementioned cases with a foreign element;
- analyse the Wassenaar Arrangement on Export Controls for Conventional Arms and DualUse Goods and Technologies, its content and its implementation in relation to spyware;
- examine the Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) and analyse its application in relation to spyware;
- examine which legal, political, diplomatic, economic or other actions, measures, remedies and sanctions the EU, its Member States and citizens could take in relation to the above categories of cases of surveillance involving a foreign element, including in relation to Area of Freedom, Security and Justice cooperation, security cooperation and other areas of cooperation;
- examine the relevance of the Commission 2021 Proposals for a Directive on Corporate Sustainability Due Diligence and on Corporate Sustainability reporting to the matters discussed in the study;
- make recommendations to the EU and its institutions, to Member States, to stakeholders, to international organisations, on the issues examined in the study.

The main objectives of the original study on digital technologies as a means of repression and social control published in April 2021 were to provide:

- an overview of the normative framework as regards the human rights standards to be respected in the use and regulation of digital technologies, as established by regional and international human rights bodies as of 2020;
- an assessment of the existing EU policy framework and toolbox to respond to the use of digital technologies for repression and control in third countries;
- recommendations for EU institutions, and the European Parliament (EP) in particular, on how the policy framework and the toolbox could be further developed to take into account current geopolitical trends and challenges to the multilateral system.

The main findings from this study derive from in-depth desk research and a series of interviews with representatives from institutions (EU, international), civil society and the private sector.
Trends in the use of technologies for repression and social control

The proliferation of new and emerging technologies has significantly expanded states’ toolkit for repression and social control, leading to gradual deterioration of the level of human rights protection in this area over the past two decades. This process has been accelerated by the COVID-19 pandemic. While China remains the global leader in actively deploying and shaping new technologies to its own strategic advantage, harnessing these technologies to undermine human rights has occurred in all parts of the world, including less developed states to which opportunities to import ‘off-the-shelf’ solutions have become increasingly available.

The main global trend emerging in recent years is the expansion of ubiquitous data collection systems, including biometric surveillance, powered by artificial intelligence (AI) and algorithmic decision-making. It extends to a number of different fields, such as distribution of vital public services, healthcare, policing, administration of justice, education, finance, immigration, and commerce. Key challenges posed by those technologies include amplification of existing biases leading to possible discrimination and a lack of transparency resulting from a ‘black box effect’. Other trends in the use of technologies for repression and social control identified in this paper include: (i) more ‘traditional’ tools and methods for repression and social control, including internet shutdowns and other network disruptions, as well as mass and targeted surveillance; (ii) an increasing use of the ‘next generation repression toolkit’, which encompasses practices that are more difficult to detect and hold accountable for (e.g. government hacking or state-sponsored online harassment campaigns); (iii) the expansion of digital authoritarian practices outside national borders through targeting diaspora or the export of surveillance technology. The rising power of a handful of tech companies which have become the gatekeepers of fundamental rights in the digital realm poses yet another significant challenge to those rights.

The risk of using new technologies to repress or control increases, in particular, in times of political tensions, elections, protests, demonstrations, armed conflicts or other kinds of crises, such as a pandemic. Among those most targeted are typically vulnerable groups, such as human rights defenders and other civil society activists, whistle-blowers, independent journalists, women, political opposition, as well as racial and ethnic minorities. At the same time, expanding AI-driven data collection systems increasingly affects wider and harder to delineate categories of victims, among whom the most severely affected are the poor and the other most disadvantage groups in the society.

Most recently, attention has focused on the spread of targeted surveillance technology, frequently used by repressive governments to track political opponents or monitor regime critics. NSO Group’s Pegasus software has been linked to over 1,000 targets in over 50 countries. While headlines have focused on Pegasus, a range of other commercial firms based in both democracies and authoritarian states -- such as Cytrox, Cyberbit, Black Cube, Cellebrite, and RCS Labs -- provide invasive tools to security services, intelligence agencies, and police departments, in pursuit of repressive objectives. In the last few years, the number of countries procuring intrusive software has risen significantly. Governments have not stopped the use of spyware due to a combination of geopolitical and commercial considerations, as well as regulatory loopholes.

The identified trends reflect a number of wider mega-trends. First, regimes’ use of state of emergency provisions related to different kinds of crises to justify long-term restrictions on fundamental rights. Second, ‘technological solutionism’, wherein technology is seen as the only viable option to resolve any social issue, often without appropriate fit-for-purpose and proportionality assessments. Third, ‘surveillance capitalism’, based on the invasive harvesting of personal data for profit by private actors, while at the same time allowing state authorities to exploit their services to their own advantage.
Recent developments in the human rights framework

Recent developments in the human rights framework reflect a growing awareness among the international community of how technologies affect societies in almost every part of our day-to-day lives. It has been widely recognised that general human rights treaties apply to the internet and other digital technologies and that design, development and deployment of those technologies are subject to a ‘three-part test’, i.e. must meet criterion of legality, pursue a legitimate aim, as well as be necessary and proportionate to achieve this aim. This means, in particular, that the use of digital technologies interfering with human rights must be always the exception, rather than the rule, must be provided in law, must be applied only in specific circumstances, and must involve the least restrictive means possible.

At the same time, the existing legal framework developed by intergovernmental bodies, both at the international and regional levels, such as the United Nations (UN), Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), Organization of American States (OSCE) and the African Union (AU), already specifically responds to many of the challenges identified above, both with its binding and (mainly) ‘soft law’ instruments. These standards are often complemented by the jurisprudence of the international courts.

Among the new and emerging technologies which may be used for repression and social control, a concern that dominates most current agendas of human rights organisations are threats posed by AI and algorithmic decision-making systems. Moreover, the human rights legal framework provides standards addressing problems such as internet shutdowns and other network disruptions, mass and biometric surveillance, government hacking, export of surveillance tools, and cyber harassment. Unfortunately, the continuing and increasing prevalence of these threats prevents them from disappearing from the human rights community’s agenda. Furthermore, several bodies developed guidelines addressing many challenges posed by tech-focused responses to the COVID-19 crisis. The important next step however, is a further assessment of the expending pandemic-related measures’ impact on human rights, ensuring they remain temporary, as well as continuing work towards more evidence-based recommendations on health emergency tools to prevent future abuse of surveillance technologies.

At the same time there are fields that should be further improved or addressed. The existing human rights framework, for instance, tackles new and emerging technologies being used for repression and social control in a fragmented way, often without taking into consideration interrelations between them. Furthermore, while there has been increasing recognition that new and emerging technologies affect not only a wide range of civil and political rights but also economic, social and cultural rights, the latter should still be given more prominence on future human rights organisations’ agendas. An ineffective application of the human rights framework at the national level, with limited avenues for remedies for harms caused by its violations, also raises concerns. A growing problem relates to the proliferation of commercial spyware used by governments to spy on human rights activists, journalists, civil society, opposition politicians, and ordinary citizens. Certain firms, such as NSO Group and Intellexa/Cytrox, have profited immensely from opaque contracts in the millions of dollars signed with law enforcement agencies that allow operators to access private communications, data, and information. There is little oversight over these activities; spyware vendors fail to conform to basic

---

1 An example may be the recent UN Human Rights Council Resolution on Freedom of opinion and expression which fails to address the impact of surveillance technologies which cause significant chilling effect on freedom of expression (A/HRC/44/12).
standards of privacy protections and human rights guarantees. Another issue are gaps that are still present in the current level of protection, specifically when it comes to challenges posed by AI. This includes the lack of a comprehensive, specifically AI-tailored international legal instrument (even though there are already advanced debates on how this gap could be filled\(^2\)), insufficient focus on the causes and impact of unintended bias and discrimination resulting from certain algorithmic and automated decision-making based on AI, or inadequacy of traditional notions of ‘victim’ status or ‘harm’ in the context of new, AI-driven technologies. Finally, a shift towards greater comprehensives has been also marked when it comes to the range of key actors who should be involved in responding to the challenges posed by new technologies. There has been an increasingly progressive approach in the legal framework towards human rights responsibilities of the private sector, particularly large online platforms, but also companies producing and selling surveillance equipment. However, due to the non-binding and non-ICT-sector specific character of the existing framework, largely based on the UN Guiding Principles on Business and Human Rights, its efficacy is currently limited. Ongoing efforts to develop a mandatory international legal instrument\(^3\) to regulate human rights obligations with respect to private companies should therefore be encouraged.

**Assessment of the EU policy toolbox**

Overall, the EU has moved up a gear in its efforts to tackle digital challenges, but its external toolbox has improved mainly on select elements of this; in particular, it has focused on the use of digital technologies for repression against democracy and human rights actors within civil society, the export of surveillance equipment, and the transnational use of digital tactics against the EU itself. In terms of its effectiveness, the EU has retained (and even widened) its toolbox for human rights and democracy support against an extremely challenging global backdrop in recent years. The EU’s direct financial support has also had a very clear, tangible impact in protecting many individual civil society activists from repression. The toolbox has become more comprehensive in the last several years, as the Union has added a number of different strands to its efforts against digital authoritarianism (i.e. digital-rights issues, digital elements in external funding for human rights and democracy, dialogues on online threats, EU cyber-security co-operation, a new cyber sanctions regime, building digital considerations into the EU’s electoral missions, surveillance export rules).

Still, it remains uncertain whether pushing back on restrictive measures related to democracy and human rights will also help counter digital repression abuses. It is also doubtful that focusing most of EU political aid to third countries on technical support to state institutions, or responding mainly to dramatic interruptions of democratic processes (such as obviously manipulated elections), rather than to gradual threats, are the optimal strategies for dealing with the specific challenges of digital repression.

At the same time, for all its improvements, it is clear that the EU toolbox does not yet fully cover all digital challenges that have arisen, and that more subtle forms of social control, advanced AI techniques or health-related controls have so far proven less amenable to being incorporated fully into foreign policy instruments. The challenge of digitally-led authoritarianism has continued to deepen,

---

\(^2\) For example, the CoE established the Ad-hoc Committee on Artificial Intelligence (CAHAI), which was tasked to examine the feasibility of a legal framework (including possibly a binding instrument) for the development, design and application of AI. See, CoE CAHAI, *Feasibility study*, 2020.

\(^3\) The elaboration of the Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises was mandated in 2014 by Resolution 26/9 of the UN Human Rights Council. The *Second Revised Draft* of the instrument was published in August 2020 and is undergoing negotiations. By the end of July 2021, a third revised draft text shall be presented, which will form the basis of negotiations later that year.
and regime attacks on democratic freedoms and human rights have become stronger and more far-reaching. Additionally, some of the emerging techniques of social control, health-system management, and advanced AI have not lent themselves easily to EU foreign policy tools. The EU itself has also devoted relatively limited funds for democracy and human rights, and it has not been willing to incur significant costs, in terms of letting trends in digital repression impact its commercial and strategic interests. In fact, the tensions between the EU’s digital geopolitics and its commitments to advance democracy and human rights make it unclear whether all EU institutions and governments see the surge in digital authoritarianism itself as a geopolitical issue. All this makes it difficult to achieve the desired results of EU policies and to conclude that its toolbox is fully attuned to the specific features of digital repression and contemporary democratic backsliding.

In particular, the EU toolkit needs to be strengthened and made more precisely tailored to the spyware challenge. The EU has inched towards having tighter exports controls, limits on the procurement of spyware from third countries, including non-Wassenaar countries, more accountable licensing of spyware products and foreign policy dialogues on spyware. However, while the EU has moved onto some fronts in trying to fine-tune its toolbox to catch up with the specificities of the spyware challenge, its toolbox lags behind the evolution of spyware challenges and the EU’s coverage of spyware’s wider geopolitical dimensions remains relatively limited.

**Recommendations**

In order to take the EU’s fledgling efforts against digital repression further, the following recommendations, encompassing both the international human rights framework and the EU’s foreign policy framework, are proposed:

**a. Putting more pressure on third countries:**

- Tightening the link between the EU’s restrictive measures and digital repression by invoking ‘essential elements’ clauses, referring specifically to the need to respect ‘digital freedoms and unhindered access to the internet’, to be included in all new trade agreements.
- Widening the new Global Human Rights Sanctions regime by referring more explicitly and extensively to the multiple strands of digital repression covered in this study.
- Making digital repression a more central part of EU’s high-level diplomacy and geopolitical strategies, and linking multilateral standard-setting forums and exercises to the EU’s on-the-ground political developments.
- Providing more EU resources specifically to strengthen the rights-oriented monitoring of surveillance equipment exports.
- Using the EU’s positive conditionality more systematically to leverage positive changes away from digital repression by responding with additional aid, trade, and strategic benefits to third-country governments that work with the Union to reform restrictive laws and incorporate international standards.
- Continuing and intensifying efforts to fuse the security and human rights elements of the EU’s digital strategies in its array of cyber-security work, and connecting Stratcom’s work to the core EU human rights and democracy support.
b. **Putting more pressure on private sector:**

- Increasing the EU’s pressure on private company operations in third countries by pushing them to adhere to more rigorous standards within the EU itself (e.g. through a code or set of guidelines pertinent to companies’ stances on internet shutdowns and acute forms of digital repression outside of Europe).

- Focusing more of the EU’s attention on the problem of ‘privatised censorship’ (i.e. online platforms making decisions that have negative effects on the freedom of expression) in its work on protection of civil society from regimes’ internet shutdowns and other network disruptions.

c. **Increasing resources, funding, and capacity:**

- Increasing the EU’s funding to digital empowerment projects (for example, by creating a ‘human rights and technology fund’, as suggested in the EP’s 2015 EP resolution).

- Using the EP’s position to get politicians (parliamentarians) engaged with civic initiatives as a means of amplifying their political impact, and to advocate for increased levels of support to the EED and other foundations.

- A more prominent role for the EP in pushing for the EU’s range of human rights dialogues and positions in multilateral forums to address such developments.

- Directing more of the EP's support to a large-scale expansion of the EU’s efforts to build digital elements into its EOMs – a natural area of partnership between the EP and EEAS.

- Investing more in the EU’s capacity for monitoring necessary to identify and unpack overt and more subtle forms of digital repression and stipulate how they contribute to gross human rights violations of the type that might be liable to restrictive measures.

- Appointing a formal liaison or contact point for the EU, which links together the multiple cyber-security and human rights initiatives.

- Investing more EU resources in fostering wider coalitions of engagement, for example by including other actors in particular civil society and academia in the work on human rights and new technologies and allocating adequate (human) resources, thus closing the ‘knowledge gap’ between legal/human rights and technology experts.

d. **Extending the global reach of EU values through the regulation of new technologies:**

- A strong push, by all actors in the EU, including the EP and the human rights community, for a comprehensive, binding legal instrument to address the specific challenges posed by AI-driven technologies.

- Using other EU standard-setting documents, such as a DSA-DMA package, the EDAP, or possible future instruments concerning mandatory due diligence for companies, to intensify multilateral efforts to strengthen the link between human rights and new technologies.

e. **With respect to spyware:**

- Calling for a moratorium on the export and import of spyware

- Long term tighter export controls on spyware

- New instruments for import controls on spyware
- More focus on spyware in diplomatic relations with Israel
- More focus on spyware in the Summit for Democracies
- An entity list of prohibited spyware providers
- Increased transparency on spyware
- Processes to protect victims of spyware
- Move spyware to the core of external relations frameworks
- Clarify use of conditionality regarding spyware
- Tailored funds for civil society organisations monitoring use of spyware
1. INTRODUCTION

This study is an updated version of the 2021 study on “Digital technologies as a means of repression and social control”, to which it adds considerations related to Pegasus-like spyware.

This section briefly presents the study objectives and scope, as well as the methodological approach to the research process. It also provides brief definitions of such terms as ‘Pegasus-type spyware’, ‘foreign elements’, ‘digital technologies’, ‘repression’, and ‘social control’ to delineate their meaning and place them in relation with, or differentiate them from, other relevant concepts used in this study. The latter include relatively recent concepts, such as ‘digital rights’, ‘surveillance society’, ‘digital authoritarianism’, or ‘algorithmic governance’.

1.1. Objectives and scope of the study

Digital technologies, and technologic developments in general, play an increasingly important role in ‘enabling and ensuring the fulfilment [of] and full respect for human rights and fundamental freedoms’\(^4\), as they provide an additional platform for their fulfillment. At the same time, they can also be abused to consolidate power and violate various dimensions of human rights. While the focus of the original study was on the use of digital technologies as a means of repression and social control, and the EU’s external human rights policy options to tackle this threat, the updated version aims at addressing the use of Pegasus-type surveillance spyware and possible policy and legislative responses to the threat such use poses. Altogether, the updated study aims to:

- describe the most important and sufficiently documented cases of alleged or confirmed use of Pegasus and of similar spyware with foreign element at global;
- examine the international, European and EU legal and policy framework on human rights (including privacy and data protection), its relevance and applicability to the production, trade and use of spyware in the various abovementioned cases with a foreign element;
- analyse the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies, its content and its implementation in relation to spyware;
- examine the Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) and analyse its application in relation to spyware;
- examine which legal, political, diplomatic, economic or other actions, measures, remedies and sanctions the EU, its Member States and citizens could take in relation to the above categories of cases of surveillance involving a foreign element, including in relation to Area of Freedom, Security and Justice cooperation, security cooperation and other areas of cooperation;
- examine the relevance of the Commission 2021 Proposals for a Directive on Corporate Sustainability Due Diligence and on Corporate Sustainability reporting to the matters discussed in the study;
- make recommendations to the EU and its institutions, to Member States, to stakeholders, to international organisations, on the issues examined in the study.

---

\(^4\) European Parliament resolution of 8 September 2015 on ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’ (2014/2232(INI)).
In order to address these, the study first explores the context of the problem of using digital technologies as a means of repression and social control, and highlights the main political and technical trends regarding human rights and digital technologies since the EP’s 2015 ‘Study on Surveillance and Censorship: The impact of technologies on human rights’\(^5\) and resolution on ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’\(^6\).

These trends are reviewed in line with the following thematic areas, presented in Chapter 2:

1. The expansion of widespread biometric surveillance and algorithmic decision-making;
2. The emergence of public health surveillance systems;
3. Digital tools of information control;
4. The next generation repression toolkit;
5. Transnational dimensions of digital repressions;
6. Pegasus and equivalent surveillance spyware.

Then, an overview and analysis of international human rights standards regarding digital technologies is presented, including standards set through relevant conventions and treaty bodies at international and regional level, advice and guidance documents adopted by special procedures and other relevant human rights mechanisms or bodies, as well as any relevant technical organisations. In this context, relevant international (governmental, private, or multi-stakeholder) initiatives that address and regulate human rights implications of digital technologies are also looked at (Chapter 3). A subsequent description and systematic assessment of the EU policy framework and toolbox for addressing the use of digital technologies for repression and social control in third countries covers:

1. Diplomatic tools at bilateral and international level;
2. Financial and technical support for reforms (governments, parliaments);
3. Support for human rights defenders and democracy activists;
4. Cooperation with the private sector, including in relation to technical standards;
5. Standard-setting in terms of businesses’ human rights obligations (due diligence);
6. Trade/export controls.

These themes were assessed according to pre-defined criteria, such as comprehensiveness, effectiveness, efficiency, availability of expertise and resources, and adequacy of the instruments aimed at authoritarian regimes. How the instruments can be applied in countries in transition/new democracies, or democratic countries at risk of backsliding, was also considered. In Chapter 4, a separate section was included to address possible legal, political, diplomatic and economic measures the EU and its Member States could take in relation to the use of Pegasus-like spyware.

Finally, based on research findings, the study offers a set of conclusions, and proposes recommendations for EU institutions – the EP in particular – on how the policy framework and toolbox


\(^6\) European Parliament, Resolution of 8 September 2015 on ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’ (2014/2232(INI)).
could be further developed to take into account current geopolitical trends and challenges to the multilateral system.

The research did not cover situations inside the EU and the EU’s internal policy framework, as it was to look at external policies. Also, the use of digital technologies for creating or disseminating disinformation was given less weight, since it is covered by another research requested by the EP.

1.2. Definitions of key concepts

The study focuses on digital technologies, which are most commonly associated with smart, high-tech, internet-based solutions and tools. As these are subject to constant improvement and new technological applications, they may, *inter alia*, include:

- Internet-based platforms and tools;
- telecommunications and video surveillance technologies (e.g. CCTV cameras);
- online databases and data pooling tools;
- Artificial Intelligence (‘AI’) based technologies;
- biometric technologies (e.g. facial recognition or finger/hand-scans);
- location technologies (e.g. Global Positioning System (GPS) or Geographical Information Systems (GISs);
- big data analytics and advanced algorithms;
- multi-level customer interaction and customer profiling;7
- Pegasus and equivalent surveillance spyware.

In this paper, the term ‘digital technologies’ is used in subsequent sections interchangeably with notions such as ‘new technologies’ or ‘emerging technologies’.

While acknowledging their wide application for the benefit of societies and human rights, the study is concerned with the use of digital technologies for repression and social control, including the use of Pegasus-type spyware systems. All the terms are further discussed below, but they essentially entail a range of negative impacts on, or threats to, the enjoyment of human rights. In the context of the digital age, human rights are also referred to as ‘digital rights’, and we use the terms interchangeably. Our understanding of digital rights thus follows a broad definition of the term as human rights that are applicable in the digital sphere. The digital sphere, in turn, ‘covers both physically constructed spaces, such as infrastructure and devices, and spaces that are virtually constructed, such as online identities and communities’8. For practical reasons, in the following chapters, we highlight human rights which are (or have the potential to be) most visibly affected in the digital sphere. This includes civil and political rights (e.g. freedom of expression, the right to privacy, freedom of assembly, the right to public participation, and prohibition of discrimination), but also – in light of the increased application of digital technologies in various sectors of life – economic, social and cultural rights (e.g. the right to work, the right to social security, the right to the highest attainable standard of health, the right to education, and the right of everyone to enjoy the benefits of scientific progress and its applications).

---


8 Digital Freedom Fund.
Given the universality, indivisibility, inter-relatedness and interdependence of all human rights, this study takes the view that digital technologies can negatively affect the full spectrum of currently recognised and newly emerging human rights.

Developments in the digital sphere have affected the functioning of states and ways in which authorities interact with citizens. The rapid growth and deployment of a new generation of AI algorithms and products has been playing an increasingly important role in public authorities’ decision-making processes. In an attempt to grasp this phenomenon, a concept of algorithmic governance has been developed, which applies to the usage of algorithms and AI-based technologies for governance purposes. This emerging proliferation of algorithms in public policy- and decision-making contributes to the creation of large data sets, updated in real time, which are increasingly being used to nudge, bias, guide, provoke, control, manipulate and constrain human behaviour.

Developments in the digital technologies can be misused as tools for human rights violations, including by governments and law enforcement bodies. Such occurrences in the context of repressive regimes lead to the development of digital authoritarianism – a concept that can be understood as ‘censorship going online’, which may include application of digital technologies to ‘control, repress, and manipulate domestic and foreign populations’ for the purpose of power consolidation. Expanding synergies between different technologies allows repressive regimes to further strengthen surveillance, societal control, or even repression. It may also bring about the usage of tools that are yet to be developed.

Digital authoritarianism is closely linked to the emergence of surveillance society, which is ‘organised and structured by using surveillance-based techniques’. Development of digital technologies not only enables wider and more intrusive access to information about people’s movements, activities or preferences, but it also provides tools to maintain, sort, and categorise data for the purposes of public decision-making and social control. This is additionally reinforced by the ubiquity of surveillance.

---

14 European Parliament resolution of 8 September 2015 on ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’ (2014/2232(INI)).
19 Ibidem., p. 5.
technology and diverse range of data available\textsuperscript{20}. An external aspect of social control could entail direct actions targeted at imposing desired behaviours of individuals and groups (as opposed to an internal social consensus that develops norms and behaviours to be followed). This can involve an active role of public institutions\textsuperscript{21} and, in some cases, some form of coercion\textsuperscript{22}. Therefore, it can play an important role in surveillance society where data-based institutional decisions can entail ‘entitlement and access to benefits, work, products and services and criminal justice; health and well-being and movement through public and private spaces’\textsuperscript{23}. This creates both incentives, and threats of possible ‘soft punishments’ for certain actions, thus providing very measurable tools for social control to reinforce or impose certain behaviours, values and norms\textsuperscript{24}. Further development and solidification of the surveillance society can, in the long-term, impact (if it has not yet done so) the agency and the autonomy of individual choice\textsuperscript{25}.

Unlike social control, repression is associated with direct targeting of certain groups or individuals (based, for example, on the likelihood of them opposing the government). In these terms, digital technologies give regimes the power not only to react to online actions, but also to carry out online tracking and to prevent any possible actions against their rule in the very preliminary phases of organising dissent\textsuperscript{26}. Techniques of repression can go beyond the online, into the real world. These could include:

- targeted censorship;
- social manipulation and harassment;
- cyber-attacks and bullying;
- purposeful internet shutdowns/slowdowns;
- penalisation of online activity and targeted persecution against online users;
- extra-legal intimidation;
- imprisonment;
- physical violence;
- other possible forms of harassment\textsuperscript{27}.

In this context, spyware surveillance, epitomised by the spread of NSO Group’s Pegasus software, is playing a growing and dangerous role in facilitating repression. Governments have repeatedly misused Pegasus to target human rights defenders, journalists, lawyers or opposition politicians in a number of states across the globe (including EU Member States such as Greece, France, Latvia, Poland and the

\textsuperscript{21} Ibidem.
\textsuperscript{22} Ragneneda M. (2011), op. cit.
\textsuperscript{24} Ragnedda, M., op.cit.
\textsuperscript{26} Tiberiu, D. And Lupu, Y., op. cit.
Netherlands)\textsuperscript{28}. But the field is not limited to Pegasus, other commercial spyware vendors, such as Cytrox, Candiru, RCS Labs, and Cyberbit have been linked to the commission of grave human rights harms as well. Spyware belongs to a category of tools classified as intrusion software, which are designed to manipulate software, computer systems, mobile devices, or networks in order to access and extract data and information\textsuperscript{29}. Unlike mass surveillance, for example, which states deploy towards a wider range of individuals or groups in an undifferentiated manner, the key distinguishing factor for spyware is that it involves targeted deployments of malware or spyware against specific individuals to collect and manipulate data and information – whether siphoning contact lists, accessing private texts and emails, grabbing location history, obtaining incriminating photos and videos, or manipulating subsequent online communications. The study examines cases involving the use of surveillance spyware, including but not limited to Pegasus software. The scope of the analysis focuses on cases with a foreign element, i.e. cases of spyware produced in a non-EU country, used by a non-EU country, or targeting non-EU citizens and examines how such software is used.

1.3. **Note on methodology**

The methodological approach to the research process included the following elements:

1. Revision of a wide range of available sources (no more than five-years-old), including:
   - official EU legal and policy documents;
   - subject-relevant international human rights ‘hard’ and ‘soft’ law;
   - subject-relevant publications by international organisations working on human rights and their bodies/mechanisms;
   - academic and grey literature focused on digital technologies and rights;
   - jurisprudence;
   - publications from established and independent media channels that display a high level of reporting on digital technologies and human rights.

2. Stakeholder consultations, based on topic guides tailored to different respondent categories, which targeted respondents from the following groups\textsuperscript{30}:
   - CSOs or their coalitions, working on human rights and digital technologies;
   - EU institutions – in particular, representatives of the EC;
   - CSOs or their coalitions, supporting human rights defenders (HRDs) and other groups affected by digitally-mediated repression and attempts at social control;
   - representatives of the private sector, particularly ICT companies;
   - representatives of international organisations\textsuperscript{31}.

---


\textsuperscript{30} No responses were obtained from representative of EU foreign policy think tanks and journalists working at the cross-section of human rights and digital technologies who were also contacted during the research process.

\textsuperscript{31} Annex 1 presents the list of consulted stakeholders and topic guides.
The main goal of the interviews was to reach a better understanding of the practice, including how the EU foreign policy framework and toolbox are employed in selected third countries, and thus, to offer an “insider” perspective on the research subject.

Since the aspiration of the research was to see how the toolbox is applied in practice on the ground, some interviews had a specific country-focus. The selection of countries, which serve as practical examples, was based on the following criteria:

- extensive use of digital technologies for repression and social control;
- different levels of democratisation/freedom, including both authoritarian and democratic states, and those in transition;
- geographic distribution, meaning countries located in different continents and regions, representing different ‘spheres of influence’.

While not fully representative, the choice of country examples aims to offer varied illustrations of trends and an opportunity to examine the application of different EU tools at country level. Overall, six countries from four continents (Africa, Asia, Europe, and South America) were selected as primary choices for more in-depth exploration. Some other criteria included participation in the Media4Democracy Technical Assistance Facility, application of EU foreign policy tools, and the presence of different trends in the employment of digital technologies for repression and social control.

In terms of its limitations, the research was centred on situations outside of the EU and on the EU’s external policy framework, referring to EU internal policies and regulations only where relevant for bilateral and multilateral relations. Also, given its global geographic coverage (minus the EU), the study cannot claim to be exhaustive in terms of its review of trends and applications of the EU foreign policy toolbox. To address this, a deliberate effort was made to balance a broad analysis that included countries representing different continents and regions with attention to the areas where the most problems lie (i.e. countries, which lead the way, in terms of using digital technologies for repression and social control). These include, in particular, regimes in China and Russia, but also in other states and under other governments, which either follow in their footsteps, or implement their own agendas reliant on digitally enabled repression and/or social control.

The update of the study follows the same methodology as the initial study. The research process was overwhelmingly based on the desk research and supplemented by the interviews.
2. TRENDS IN THE USE OF DIGITAL TECHNOLOGIES FOR REPRESSION AND SOCIAL CONTROL

The following chapter will map the current global trends related to the use of new technologies for repression and social control. It will present an overview of how digital repression and social control have evolved in recent years, and how they currently work across the world – in particular, which regimes engage in such activities, and using what methods and tools. It will also explain how these efforts impact human rights, identify the most targeted or vulnerable groups, and highlight what the role of private sector is in the context of this phenomenon.

2.1. Expansion of widespread biometric surveillance and algorithmic decision-making

The year 2020 has brought an unprecedented rapid upscaling of new technologies that support digital surveillance, in response to the COVID-19 pandemic. Governments across the world have deployed a range of new surveillance measures, often turning to advanced AI and big data technologies, used not only for enhanced monitoring, but also increasingly to replace human judgment with algorithmic decision-making. Applications of these technologies may affect a particularly broad spectrum of human rights, ranging from the right to privacy, freedom of expression, freedom of peaceful assembly and association, and the right to non-discrimination to a number of social and economic rights, such as the right to health, work, and social security. While in principle all regions have witnessed the expansion of tech-focused responses to the pandemic, the countries that have been leaders in harnessing the most sophisticated technologies to combat COVID-19 were often the same states where intrusive, data-driven surveillance systems were in place even before the COVID-19 crisis began. The pandemic has therefore served as a catalyst for expanding those systems, while also preserving many pre-existing problems related to their use.

China is the country with the most advanced and pervasive surveillance system, built over the past two decades. It has also taken the most comprehensive and draconian approach to COVID-19 surveillance. Categorised as ‘the world’s worst abuser of internet freedom for the sixth year in a row’ according to Freedom House’s ‘Freedom of the Net 2020’ report, China has been the leader in the application of biometric surveillance, which is particularly ubiquitous in northwest China’s Xinjiang Uyghur Autonomous Region. Chinese authorities use biometric identification to track and restrict the

---

33 AI is a broad concept used in policy discussions to refer to many different types of technology. To date, there is no single definition of AI accepted by the scientific community. Definitions used by international organizations also vary. A comprehensive document on the definition of AI has been published by the High-Level Expert Group on AI mandated by the European Commission. See: AI HLEG, ‘A Definition of AI: Main Capabilities and Disciplines’, 2019.
34 Freedom House, 2020, op. cit., p. 2. The Report determines each country’s internet freedom score on a 100-point scale, based on 21 indicators pertaining to free flow of information online and deployment of new surveillance technologies by public and private actors, which to great extent correspond to the concepts of ‘surveillance’ and ‘social control’ as used in this study.
35 Xinjiang is an autonomous region in China which is home to a number of ethnic minorities, including the Muslim Uyghur minority, a Turkic ethnic group, recognized as native to the Region. The Chinese government has long carried repressive policies in Xinjiang, maintaining its actions are justifiable responses to a threat of extremism due to the East Turkestan independence movement (a political movement that seeks independence for the Region). These efforts have been dramatically scaled up since late 2016, when Communist Party Secretary Chen Quanguo relocated from the Tibet Autonomous Region to assume leadership of Xinjiang. At the same time human rights organisations and experts have presented evidence that these policies involve gross human rights violations, including mass arbitrary detention, torture, surveillance and mistreatment of Turkic Muslims in Xinjiang. See: Global coalition of more than 300 civil society organisations, ‘Global call for international human rights monitoring mechanisms on China. An open letter to: UN
movements and activities of the Uyghur through the use of facial recognition technology and mandatory collection of sensitive data, such as DNA samples and iris scans. It has also been established that this surveillance technology is used to arbitrarily place large numbers of Uyghurs and members of other ethnic groups in so-called ‘re-education camps’ under the pretext of countering religious extremism, without detainees being charged or tried. As noted by the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, ‘the picture that emerges [from the Uyghur Autonomous Region] is one of systemic ethnic discrimination, supported and indeed made possible by a number of emerging digital technologies’.

Algorithmic technologies based on big data have also been deployed in other parts of China. The authorities have been experimenting with machine learning and algorithmic decision-making in the service of the regime’s politically repressive ‘social management’ policies. Automated systems flag suspicious behaviour on the internet and, increasingly, in public spaces, using the world’s largest security-camera network equipped with facial recognition, which enables tracking of individuals based on their physiological or behavioural characteristics. Data sets assembled through these surveillance efforts could feed into a ‘social credit’ system that creates an assessment of individuals’ online activities and other personal data to monitor and rate individuals’ overall behaviour. Being listed as a ‘problematic’ group or individual by municipal or provincial authorities, which are currently testing these systems, can result in restrictions on movement, education, and financial transactions. By contrast, people and legal entities ranked highly could win tax reductions or privileged access to governmental and private services, including deposit waivers, free library book borrowing, or shorter lines at airport security. During the pandemic, the Chinese government has combined the pre-existing monitoring apparatus and biometric records with invasive new apps and opportunities for data collection to identify potentially infected persons and enforce population quarantine (e.g. by using drones and upgrading facial-recognition cameras with thermal detection technology).

Many other governments besides the Chinese (including in countries across the democratic spectrum) have been rolling out biometric and AI-assisted surveillance with few or no protections for human rights, however. The rise of biometric surveillance, in particular facial recognition technology, can be observed in different parts of the globe, despite evidence that it may exhibit bias and lead to or

---

36 Much of the information collected through the surveillance systems is stored in a massive database, known as the ‘Integrated Joint Operations Platform’, which uses AI to create lists of ‘suspicious people’ who then may subject to detainment. Classified Chinese government documents released by the International Consortium of Investigative Journalists (ICIJ) in November 2019 revealed that more than 15,000 Xinjiang residents were placed in detention centres during a seven-day period in June 2017 after being flagged by the algorithm. The detainees seem to have been targeted for a variety of reasons, including traveling to, or contacting people from, any foreign countries China considers sensitive, attending services at mosques, having more than three children, or sending texts containing Quranic verses. The Chinese government called the leaked documents ‘pure fabrication’ and maintained that the camps are education and training centers. See: UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, ‘Racial discrimination and emerging digital technologies: a human rights analysis’, A/HRC/44/57, 18 June 2020, par. 39.; Maizland, L., ‘China’s Repression of Uyghurs in Xinjiang’, Council on Foreign Relations, 1 March 2021.; Allen-Ebrahimian B., ‘Exposed: China’s Operating Manuals for Mass Internment and Arrest by Algorithm’, International Consortium of Investigative Journalists, 24 November 2019.

37 Ibidem.


reinforce discrimination\textsuperscript{41}, alongside being intrusive in nature, lacking regard for privacy. The countries that have recently been expanding facial recognition cameras in public spaces, for example, include Kyrgyzstan\textsuperscript{42}, India\textsuperscript{43}, a number of Latin American countries\textsuperscript{44}, as well as some ‘Global North countries’ such as Israel (which has implemented the system on the West Bank)\textsuperscript{45}, the United States\textsuperscript{46}, and Australia\textsuperscript{47}. The most prominent example of AI-assisted surveillance is Russia, where the pandemic has accelerated a process of installing a network of 100,000 facial recognition cameras to keep track of quarantined individuals\textsuperscript{48}. The expansion of this technology has contributed to the regime’s already pervasive surveillance mechanisms based on, among others, pre-existing and ever-expanding laws allowing for mass surveillance and curbing of internet freedom\textsuperscript{49}. These developments increase the authorities’ capability to monitor both online and offline spaces and facilitate targeting of peaceful protesters, cracking down on critical media and repressing civil society organisations. They also enhance the government’s capacity to conduct fine grain censorship\textsuperscript{50}.

The expansion of algorithmic decision-making systems, including those processing biometric data or making inferences about sensitive personal data, extends to a number of different fields, including distribution of public services, social security, healthcare, policing, administration of justice, education, finance, immigration, and commerce. In the criminal justice context, for example, police departments in different parts of the world (e.g. the United States, China, India) have been using emerging digital technologies for predictive policing\textsuperscript{51}, whereby AI systems pull from multiple sources of data, such as criminal records, crime statistics and the demographics of neighbourhoods\textsuperscript{52}. Another example may be drawn from the area of social security. The use of digital technologies has contributed to the emergence of a so-called ‘digital welfare state’ in many countries across the globe, a trend considered to provide ‘endless possibilities for taking surveillance and intrusion to new and deeply problematic heights’\textsuperscript{53}. This particularly applies to the development of digital identification systems that involve the collection of various forms of biometric data and are used to determine the distribution of social benefits and access to public services (see Box 1). Governments that have been experimenting with incorporating these technologies into their welfare systems include:

- India;


\textsuperscript{44} Interviews with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020 and Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now, 6 January 2021.

\textsuperscript{45} Ziv, A., \textit{This Israeli face-recognition start-up is secretly tracking Palestinians}, Haaretz, 15 July 2019.


\textsuperscript{47} Bivas, J., \textit{Facial recognition system rollout was too rushed, Queensland police report reveals}, ABC, 5 May 2019.

\textsuperscript{48} BBC, \textit{Russia: Moscow uses facial recognition to enforce quarantine}, 3 April 2020.

\textsuperscript{49} Claessen, E., \textit{Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU}, Journal of Cyber Policy, 5(1), 2020; European Court of Human Rights, ‘Zakharov v. Russia’, No. 47143/06, 4 December 2015.; Human Rights Watch, \textit{Russia: Social Media Pressured to Censor Posts}, 5 February 2021. See also Figure 5 and 6.

\textsuperscript{50} Human Rights Watch, \textit{Russia}, 2020; Activists A. Popova and politician V. Milov have lodged a complaint over Russia’s use of facial recognition technology during protests to the European Court of Human Rights. This will be likely the first case challenging the use of facial recognition technology to conduct mass surveillance in the court’s practice.

\textsuperscript{51} Automated predictions about who will commit crime, or when and where crime will occur.


All these algorithmic systems raise grave concerns, as the basis for their decision-making is opaque, but opportunities to appeal and get redress in cases of abuse are very limited, if existent at all. There is also a risk that many of the data sets fuelling these systems reflect existing racial or ethnic bias, despite the presumed ‘objectivity’ of these technologies. It has been established that they can operate in ways that reinforce discrimination and cause serious harm, in particular to people from certain racial or social groups (such as people with non-white faces, or the poor). In the law enforcement sector, errors may lead to false accusations and arrests. In the context of distribution of social welfare, they may result in unjustifiable loss of benefits or reduced access to services, and eventually contribute to reinforcing social inequalities.
Box 1: Examples of algorithmic harm

**Predictive policing**

The ‘Correctional Offender Management Profiling for Alternative Sanctions – COMPAS’ system is a notorious example of an AI system with discriminatory effects. It is a scoring tool used in some states in the United States (US) to assess the risk of someone committing a crime, with the aim of helping judges to determine whether they should be allowed to go on probation. While the system did not directly consider the racial origin or skin colour of the assessed person, a detailed analysis of the results showed that black people were more often rated as risky in terms of committing a crime than white people.

**Digital identification systems**

The world’s two largest digital identification systems are ‘Huduma Namba’ in Kenya and ‘Aadhaar’ in India. Among other data, they involve the collection of fingerprints, retina and iris patterns, voice patterns, and other identifiers. They determine access to essential government services (such as voting, registering birth certificates and civil marriages, or paying taxes) or access to pensions and unemployment benefits. However, there is evidence that, ‘when trying to access public services through these systems, certain racial and ethnic minority groups in both countries find that they are excluded, while others face logistical barriers (...) that in effect can result in de facto exclusion from services to which they are entitled’. Furthermore, people with disabilities have ‘experienced discrimination for not being able to provide fingerprint or iris scans’.

### 2.2. Emergence of public health surveillance systems

Apart from the expansion of existing surveillance systems, the COVID-19 crisis has also led to the unveiling of many high-tech tools specifically aimed at tackling the pandemic. The most prominent example is a rapid rollout of pandemic-related mobile applications used for contact tracing, quarantine enforcement, social distancing monitoring, or symptom tracking, sometimes combined with a health status code. Such smartphone apps have been introduced in at least 54 countries across the globe.

These technologies may offer benefits to policymakers, the medical community, and to society at large (for example, by supporting efforts to protect public health and manage the crisis), but their widespread application also carries significant implications for fundamental rights. In many instances, these tools have been developed with minimal protection against abuse (such as excessive use by law enforcement agencies for non-pandemic-related purposes), without sufficient evidence to confirm their efficacy to protect public health or appropriate scrutiny into whether they are proportionate to counter-epidemic efforts. Even though the use of mobile location data may reveal sensitive information about people’s identity, location, behaviour, associations, and activities, many developers have largely ignored principles of privacy-by-design, which would ensure that privacy considerations are built into a tool’s architecture and software. Apps are often closed sourced, centralised (sending

---

57 UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, op. cit. par. 40. UN Special Rapporteur on extreme poverty and human rights, op. cit., par. 15.
58 UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, ibidem.
unencrypted data to centralised government servers) and with insufficient cyber-security standards, allowing data to be shared with multiple institutions. This is particularly problematic in the case of repressive regimes, where human rights defenders, independent journalists, or opposition leaders are routinely targeted, as apps that generate sensitive health and social networking data about these individuals increase opportunities for abusive surveillance. Moreover, in some countries (Singapore, Ukraine, and Bahrain, for example) apps have been made mandatory, having a disproportionate and discriminatory impact on certain populations, particularly when non-digital alternatives are not provided (see Table 1). In other countries, such as China, India, and Turkey, COVID-related health status and contact-tracing mobile apps, even though not officially mandatory, have been made gatekeepers for access to essential public services, such as public transport and other public spaces, workplaces or shopping malls.

Table 1: Examples of human rights implications of mandatory pandemic-related apps

<table>
<thead>
<tr>
<th>Country</th>
<th>Type of application</th>
<th>Problem</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singapore</td>
<td>Contact-tracing app</td>
<td>Discriminatory impact</td>
<td>The app is obligatory for some categories of migrant workers who already faced discrimination, increasing the risk of further marginalisation of this group.</td>
</tr>
<tr>
<td>Ukraine</td>
<td>Quarantine-enforcement app</td>
<td>Discriminatory impact and Risk of exposure to life-threatening situations</td>
<td>The government required people crossing its borders to install the app to monitor compliance with self-isolation orders. This has particularly affected elderly people in the Donetsk region, where many are unable to download the app and are therefore denied entry to government-controlled territory, instead left stranded in an active conflict zone.</td>
</tr>
<tr>
<td>Bahrain</td>
<td>Quarantine-enforcement app</td>
<td>Excessive punishment</td>
<td>Individuals failing to comply with the obligation to use the mandatory app and wear the electronic wristband which comes with it face severe criminal sanctions (up to 26,000 USD fine and/or a minimum three-month jail term).</td>
</tr>
</tbody>
</table>

Data-driven responses to the pandemic are not limited to mobile apps. In different parts of the world, they also include solutions such as digital permit systems for non-essential travel, both on public transport and in private vehicles (Russia); expansion of state access to data stored by telecommunications companies (in at least 30 countries across the world); and the aggregation of data on new public health platforms from different sources. The last two measures have been deployed

---

in Ecuador, where the government has introduced laws enabling satellite tracking of people suspected of having COVID-19 to ensure that they are complying with isolation requirements, and has also established a platform aggregating location data, surveillance camera footage, and data from a symptom-checking app⁶⁷.

Overall, the pandemic has likely led to the emergence of new ways of ‘digital social sorting, in which people are identified and assigned to certain categories based on their perceived health status or risk of catching the virus’⁶⁸. It has also exposed the problem of public-private partnerships in the area of surveillance, as many governments have provided their pandemic-related technological solutions in collaboration with private companies that develop surveillance tools or process user data (such as telecom companies or internet service providers). This illustrates a wider trend of ‘outsourcing’ surveillance by states, often with very little transparency and in cooperation with companies ‘hiding’ behind confidentiality and trade secret exceptions⁶⁹. When those partnerships are implemented without appropriate safeguards and public oversight⁷⁰, it increases the risk of extending over governments’ capability to exploit citizens’ data, and also provides private corporations with more opportunities to monetise it. Furthermore, sudden proliferation of pandemic-related apps may contribute to ‘normalisation’ of widespread digital surveillance, especially as many opaque systems of information collection and predictive analytics have been implemented under the guise of emergency measures, with very little public scrutiny or debate, limiting public awareness of their potential negative and long-term implications⁷¹.

2.3. Digital tools of information control

Government-imposed restrictions on electronic communication, such as network disruptions, the shutting down of internet connectivity, bans on entire social networks and applications, or suspension of telephone services, as well as more targeted censorship (like individual website blocking or filtering specific content), are on the rise globally and continue to be an alarming threat to human rights⁷². While they affect freedom of expression, in particular (just as in the case of widespread surveillance), they also interfere with multiple other rights, such as the right to association and peaceful assembly, public participation, privacy, and non-discrimination. The COVID-19 crisis has highlighted their impact on economic, social and cultural rights, as online access to healthcare, education and other essential services, for many people, has become the only viable option.

---


Internet shutdowns remain one of the most common tools for digital repression, continuing to be used by many governments in different parts of the world to silence dissenting voices, often during critical events, such as protests and demonstrations, elections, or armed conflicts. Internet shutdowns dominate in developing and/or non-democratic countries, where relevant protective legal provisions are non-existent or limited and rarely acted upon. Overall, at least 213 shutdowns were documented in 2019 in 33 countries (India being the current evident ‘leader’, with at least 385 shutdowns ordered since 2012, followed by Venezuela, Yemen and Iraq). This number stands in stark contrast to 2015, when ‘only’ between 15 and 33 major disruption episodes were registered. Not only have shutdowns been rapidly increasing in number (see Figure 1), but they have also lasted longer and affected more people, especially from vulnerable groups. This is visible, above all, in Africa, where the number of internet shutdowns grew by 47% between 2018 and 2019, and is still on the rise. In Asia, where they are also frequent, shutdowns increasingly target refugees or other minority populations (for example in Myanmar, Bangladesh, India, and Indonesia). Unfortunately, the increasingly severe impact of internet shutdowns on human rights has been additionally exacerbated by the COVID-19 pandemic (see Box 2).

While there is no academic unanimity on the definition of the term ‘internet shutdown’ and many sources use it interchangeably with ‘network shutdown/disruption’ or ‘blackout’, for the purpose of this study we will use a definition developed by Access Now, one of the main advocacy organisations monitoring this problem across the world, which has defined it as ‘an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information’. Access Now, ‘Keep It On Report 2019’, 2020, p. 2.

In 2019, the most commonly observed causes were protests, military actions (mostly in India), communal violence, political instability, religious holidays or anniversaries, and elections, with an aim to undermine collective reaction to those events. Interestingly, the evidence suggests that the ‘effectiveness’ of shutdowns is questionable at best – i.e. that shutdowns are frequently followed by an escalation in the momentum of pre-existing protest, and that activists and citizens use a combination of strategies to continue mobilising. See: Rydzak, J., Karanja, M. and Opiyo, N., ‘Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries’, International Journal of Communication, 14(2020), 2020, p. 4281.

There is, however, a significant gap between leading India and – next on the list – Venezuela, which was reported to have blocked access to social media platforms at least 12 times in 2019, equal to 86% of internet shutdowns in Latin America (the remaining 14% was attributed to Ecuador). Access Now, op. cit., pp. 2-3.

African country with the biggest number of shutdowns is Algeria (6) followed by Ethiopia (4) and Sudan (3). Giles, C. and Mwai, P., ‘Africa internet: Where and how are governments blocking it?’, BBC, 2 November 2020. Shutdowns have been imposed mainly in response to increasing volume of protests and elections-related social unrest; see: Garbe, L., ‘What we do (not) know about Internet shutdowns in Africa’, 29 September 2020.

Box 2: Implications of internet shutdowns in the COVID-19 era

Internet shutdowns have particularly detrimental effects in light of the COVID-19 crisis. The pandemic has amplified the need for access to reliable, open, secure, and affordable internet.

Intentionally degraded or shutdown internet access has impeded effective responses to COVID-19 and threatened people’s right to health. It has prevented the dissemination of health information and other crisis-related information, such as updates on government restrictions, which are critical both for the general public and for healthcare workers seeking knowledge and guidelines on treating the virus. Furthermore, blocking people from getting essential services, accessing education and/or work, conducting business, and communicating with families has affected a number of other social, economic, and cultural rights. During periods of isolation, access to all these essential services and opportunities has relied on the Internet even more than usual.

Despite these harmful effects, internet shutdowns have been imposed or continued in at least 14 countries since the crisis began (Bangladesh, Belarus, Ethiopia, India, Indonesia, Iran, Kazakhstan, Myanmar, Pakistan, Philippines, Sudan, Uganda, Zambia and Zimbabwe)\(^2\).

One of the most drastic examples of a shutdown carried out during the pandemic is the internet blackout and phone restrictions imposed by state authorities at the Rohingya refugee camps in

---

\(^1\) Ibid.; Access Now, *Keep It On Report 2018*, 2019; Rydzak, J., op. cit. The numbers refer to shutdowns that human rights organisations, such as Access Now, managed to document and verify; the actual number of shutdowns may be higher. For 2015, the available data indicates that there were between 15 and 33 major disruption episodes registered in 2015. See: J. Rydzak, op. cit.

\(^2\) Freedom House, *Freedom of the Net 2020 Report*, 2020, op. cit., p. 10; See also the Excel data for the list of countries; Access Now, *Cutting internet access when people need it the most: stories from Uganda*, 9 February 2021.
Bangladesh, which have been hindering humanitarian groups from addressing the threats posed by COVID-19.83

It should be noted that shutdowns are not always a monolithic “kill switch”, but may vary in scale, scope, location, duration, and frequency. Sometimes restrictions do not involve complete blackouts of internet connectivity across the entire country, but are targeted at a particular region or regions (e.g. recent targeted shutdowns carried out in Ethiopia in the Oromia region84, or in Myanmar in parts of the Rakhine and Chin states85). They may also constitute a more ‘subtle’ disruption in the form of deliberate slowdowns, often leading to the same practical effects as full shutdowns (e.g. after lifting a seven-month blanket internet shutdown in Jammu and Kashmir in 2020, the Indian authorities have restricted internet access to only slow-speed 2G86). Other governments ‘focus’ on online platform blocks, targeting global platforms with dominant positions on the market, which have become key channels for accessing information, in particular87. In Venezuela, for example, access to social media such as Facebook, Twitter, and Instagram was blocked at least 12 times in 201988, or most recently during the military coup in Myanmar89. Official government justifications for imposing these measures range from a need to combat fake news and hate speech, to public safety and national security. These justifications rarely match what observers conclude to be the actual cause, however90.

Other forms of restricting the free flow of information online used by governments to censor critical voices involve more targeted access restrictions, such as Internet Protocol (‘IP’) Address blocking, Domain Name System (‘DNS’) filtering, and redirection or Uniform Resource Locator (‘URL’) filtering91 (e.g. ‘the world’s most advanced apparatus for such internet censorship’ operated by China, known as the ‘Great Firewall’92). Furthermore, states are putting increasing pressure on tech companies to take down content and share user data, which can be observed in transparency reports published by large online platforms93. In 2020, this trend also involved blocking independent media websites reporting on the spread of COVID-19 to suppress unfavourable health statistics or critical reporting on

86 There have been several reports indicating that residents in Jammu and Kashmir are unable to access information about COVID-19 due to the restriction on high-speed 4G internet access in these areas. It has been also revealed that the restrictions make access to video conferencing – currently a critical lifeline throughout India and much of the world – virtually impossible; Access Now, ‘#KeepItOn: Open letter appealing to the Deputy Director-General to urge the governments of Bangladesh, India, Myanmar, and Pakistan to end the ongoing internet shutdown amid COVID-19 pandemic’, 26 May 2020.
87 See also Box 4 below for data on how global digital market is dominated by a handful of online platforms.
90 See footnote no. 66.
91 These are different, IP, DNS or URL-based online content blocking techniques which from the user’s perspective lead to the same effect, namely some parts of the internet inaccessible. For more detailed descriptions of these techniques see: Internet Society, Internet Society Perspectives on Internet Content Blocking: An Overview, 2017.
92 Not only blocking access to tens of thousands of sites and domain names, but also enabling automated and systematic internet censorship of content criticising the regime. Garside, S., Democracy and Digital Authoritarianism. An Assessment of the EU’s External Engagement in the Promotion and Protection of Internet Freedom, College of Europe - EU Diplomacy Papers 1/2020, 2020.
governments’ responses to the crisis. Censorship of COVID-19 content was registered in at least 28 countries, with most prominent examples in China, Venezuela, and Egypt94.

Other ways that governments enhance their censorship capacity include the introduction of legislation, a trend that is not new, but again amplified by the pandemic. During the COVID-19 crisis, at least 20 countries adopted new regulations, sometimes as part of state of emergency laws, through which vague and overly broad speech restrictions were imposed95. In particular, governments responded with the enactment of laws that criminalised fake news and provided excessive, harsh penalties for those found guilty of spreading it, as well as by imposing new regulations for online platforms (see Table 2).

Table 2: Examples of new laws challenging internet freedom

<table>
<thead>
<tr>
<th>Country</th>
<th>Main provisions</th>
<th>Sanctions</th>
</tr>
</thead>
</table>
| Tanzania96 | The new law:  
  • Requires that bloggers and other content providers register and pay expensive licensing fees for publishing content online  
  • Expands the list of prohibited content to include informing about deadly or contagious disease without authorities' permission  
  • Forces online services providers to filter and censor content using automated tools, such as upload filters, and requires immediate takedown of alleged illegal content without due process safeguards | A person who publishes prohibited content shall, upon conviction, be liable to a fine of not less than 2,000 USD and/or imprisonment for no less than 12 months |
| Zimbabwe97 | The new law penalises false information about the pandemic98 in both online and offline (real life) environments | Fine of up to 10,000 USD and/or imprisonment for a period not exceeding 20 years |
| Russia99 | Penalise public dissemination of knowingly false information leading to grave consequences, which | Among other sanctions, a fine of 19,000 to 25,500 USD, |

95 Ibid.
97 Ibid.
98 The law penalises precisely publication or communication of false or fake news about ‘any public officer, official or enforcement officer involved with enforcing or implementing the national lockdown in his or her capacity as such, or about any private individual that has the effect of prejudicing the State’s enforcement of the national lockdown; Ibid.
Multiple internet-related laws were adopted in 2020/2021, which:

<table>
<thead>
<tr>
<th>Cause of Harm/Action</th>
<th>Legal Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>caused harm to an individual's health (criminal law)</td>
<td>correctional labour, or up to 5 years of imprisonment</td>
</tr>
<tr>
<td>Address the dissemination of false or inaccurate information by legal entities that are using mass media or the internet (administrative law)</td>
<td>A fine of up to 127,800 USD and confiscation of equipment</td>
</tr>
<tr>
<td>Penalise 'libel' committed online (criminal law)</td>
<td>A fine of up to 13,300 USD and/or up to 2 years of imprisonment</td>
</tr>
<tr>
<td>Oblige hosting providers to remove content deemed illegal under Russian law (administrative law)</td>
<td>A fine of up to 13,500 USD and, in the event of repeated offense, up to 10% of any company's annual revenue</td>
</tr>
</tbody>
</table>

Besides that, numerous states continue to take punitive actions against bloggers, journalists, activists, or whistle-blowers publishing on the Internet, often based on spurious charges of spreading hate speech or fake news. This is, again, not a new trend, but remains very present in many parts of the world. In 2020, this trend affected dissemination of credible and timely information about the pandemic in particular, which has been undermined by retaliation against political opponents, journalists, human right lawyers, and healthcare workers engaging in online discourse about COVID-19 (e.g. revealing the actual scale of the outbreak or speaking out about unsafe working conditions in the health sector). Overall, in at least 45 countries, activists, journalists, and other members of the public were arrested or charged with criminal offenses for online expression related to the pandemic, based either on laws passed before the coronavirus crisis, or on new legislation tailor-made for the pandemic. Such criminal investigations have been opened in, among other countries, Russia, Turkey, Venezuela, Tanzania, Morocco, Kenya, and China, where recently one such 'whistle-blower', Zhang Zhan, was sentenced to four years imprisonment.

Finally, in a growing number of countries, network disruptions and other repressive actions impeding access to online information have been facilitated by efforts to enhance 'sovereign control' over online information space. Multiple states have adopted measures to control the flow of data in and out of their national borders and isolate 'domestic' internet from the global network. Imposing new restrictions on cross-border data transfer and storage, as well as centralising technical infrastructure, is often justified by the authorities as responsive to the need to protect user privacy and improve cyber-security, particularly in the context of threats posed by globally-operating online platforms. In countries with no due regard to human rights, however, it may as well be used as a tool for extending surveillance and censorship through even more pervasive monitoring and filtering of all traffic coming to the country, as well as easier access to sensitive information and user data for domestic law enforcement agencies. While China and Russia have been the key driving force behind 'cyber sovereignty' (see Box 3), it has

---

100 Still, according to the Reporters Without Borders, more than a half of the world’s imprisoned journalists (61%) are being held in just five countries: China, Egypt, Saudi Arabia, Vietnam and Syria. Reporters Without Borders, ‘Round-up 2020, Journalists detained, held hostage and missing’, 2020.


recently been expanding particularly quickly in countries such as Iran, Brazil, India, Turkey, Vietnam, and states in North Africa. At the same time, it needs to be flagged that states’ efforts to increase national control over global online platforms and, more generally, over the ‘domestic internet’, albeit motivated by different intentions, have become a global trend also present in Western countries, including in the EU’s pursuit of strengthening its ‘digital sovereignty’.

Box 3: Cyber sovereignty in China and Russia

**China**

China has long pursued a cyber sovereignty agenda aimed at increasing control over ‘national’ internet with restrictive internet policies, including in particular the infamous ‘Great Firewall’. Among other limitations, those policies prevent citizens from accessing certain foreign information sources (as a result of blocking selected websites and services that the government has put on its blacklist) and force overseas tech companies to adapt to China’s domestic regulations. The 2017 Cyber-security Law expanded the cyber sovereignty trend by, among other things, requiring that critical information infrastructure operators store personal and important data domestically and make it accessible on demand to the authorities, introducing ‘security assessments’ necessary for the transfer of any such data abroad, or imposing the user real-name registration obligation by network operators. In the wider context of crackdown on internet freedom in China, these provisions are believed to further undermine human rights in digital space in the country.

**Russia**

In 2019, Russia introduced a package of laws concerning the ‘autonomous Russian internet’. The laws foresee that ‘internet traffic within Russia could only go through Internet exchange points (IXPs) that are pre-approved by the institution issuing control and supervision of the internet, Roskomnadzor’. In practice, ‘this creates a system that gives the authorities the capacity to block access to parts of the Internet in Russia, potentially ranging from cutting access to particular internet service providers through to cutting all access to the internet throughout Russia’. Such a scenario does not seem unrealistic in light of recently documented internet outages and escalating pressure on online platforms to remove content deemed illegal by the authorities, amid protests against the

---


108 Netblocks (2021), ‘Internet disrupted in Russia amid opposition protests’, 23 January.

109 One of the new laws adopted in January 2021 was already used to impose fines on a number of online platforms which were considered not to have complied with an obligation to remove illegal content related to ‘incitement to participate in the unlawful protests’. See, Roskomnadzor (2021), ‘Социальные сети будут привлечены к ответственности за
detention of prominent opposition activist Alexei Navalny, and in light of other rapidly growing concerning internet policies in Russia (see Table 2).

2.4. Next generation repression toolkit

There are also a number of fairly recent trends encompassing the ‘next generation’ of techniques used by governments to interrupt citizens’ access to online information and target their privacy, which are likely to further expand in the future. Over time, repressive regimes have developed an arsenal that extends from technical measures, laws and policies to more covert and offensive techniques including targeted malware attacks, such as Distributed Denial of Service attacks (DDoS attacks) or targeted cyberespionage campaigns. The use of such techniques was documented in most countries which, according to Freedom House’s latest ‘Freedom on the Net’ report, have the worst conditions for internet freedom, or have experienced the biggest decline in internet freedom recently. These include, among others:

- China, using malware redirecting the website requests of unwitting foreign users into DDoS attacks or replacing web requests with malicious software;
- Kyrgyzstan, where independent media websites were disabled by DDoS attacks;
- India, using spyware against prominent activists, journalists, and lawyers involved in advocating for the rights of marginalised groups;
- Nigeria, with cyberattacks targeted at independent journalists and media outlets;
- Rwanda, where spyware was used to monitor and intimidate exiled dissidents.

Sophisticated spyware attacks on human rights defenders, activists and journalists are increasingly backed up by states’ efforts to undermine the technology which provides these groups with important means to protect their security online and, in general, facilitates the exercise of human rights in a digital age. Repressive regimes respond to its use by blocking secure messaging apps, implementing so-called ‘back-door access’ in commercially available products, or introducing laws compromising user anonymity, such as limits on virtual private networks (‘VPN’), encryption or imposing real-name registration obligations.

---

110 A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. (...) A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack. See: CISA (2019), ‘Understanding Denial-of-Service Attacks’, November 20.


The next generation techniques also involve efforts to indirectly impede the free flow of information by engaging government-recruited ‘troll armies’ that, looking like spontaneous expression, use privately-owned popular online platforms to discredit or intimidate any dissenting voices or disseminate disinformation aimed at drowning out accurate content. Apart from a negative impact on the right to privacy of those targeted by such actions, their ultimate goal is often to generate a ‘chilling effect’ on freedom of expression – i.e. to discourage activists or independent journalists from using digital communication for fear that they would be monitored or intimidated. Examples of pro-government ‘e-warriors’ include India’s ‘Modi’s Yoddhas’, associated with the ruling Hindu nationalist Bharatiya Janata Party, Russia’s ‘Kremlin’s troll army’, the Brazilian ‘President Bolsonaro’s hate office’ or the Vietnamese ‘Force 47’.

While attacks on the internet target different categories of victims, one of the continuing challenges, which has been receiving increasing attention from researchers and human rights organisations in recent years has been continuing gender-based harassment, including cyber violence faced by women. Not only do women appear to be disproportionately targeted, but attacks against them often also involve particular forms of online abuse, including sexuality-related threats (such as stalking, rape threats, doxing, and non-consensual disclosure of sexually explicit images and videos). Such harassment targets, in particular, female journalists, human rights defenders who speak out against government abuses and on women’s rights issues, politicians and opposition leaders, and other women engaging in public debate, intimidating them out of the public space and spurring discrimination.

Another emerging challenge for a free flow of information online, which will likely become more ubiquitous in the future is the rise of automated censorship. This often encompasses sophisticated content filtering techniques that engage algorithms powered by machine learning and, in some parts of the world (in China, for example) already fuelling real-time censorship tools without explicit user notice (which makes it ‘more difficult to detect and react to because it is being done invisibly upstream of the user’). In a number of countries (in India, for example, or already-mentioned Tanzania) new legislation has been adopted recently obliging service providers to proactively filter online content, without sufficient safeguards preventing the possible abusive use of such tools.

At the same time, automation in content moderation has increasingly been used on a voluntary basis by the most popular global online platforms. Even when not applied with intent to silence any particular voices, it in fact ‘exposes all speech to a form of evaluation ex ante and in a way that fails to consider linguistic, social, historical, and other relevant context’. It creates substantial risks to freedom of expression, especially when coupled with a lack of due process safeguards available to users, including transparency and effective remedies. The is exacerbated by the lack of independent,

---

external oversight of platforms’ decisions and the fact that these actors, not only due to specificities of their services but also their dominant positions on the market, serve as powerful gatekeepers for public discourse and access to information (see Box 4). One of the most disturbing recent examples of such ‘privatised censorship’ carried by large tech companies concerns suppressing dissenting voices from marginalised and oppressed communities on platforms such as Facebook and Twitter in the Middle East and North Africa (MENA) region. They include arbitrary and non-transparent suspension and removal of accounts belonging to journalists and activists in Tunisia, Egypt, and Syria (some of which documented war crimes and human rights violations). The scale and frequency of these suspensions suggests that the problem likely results from algorithmic bias, rather than from isolated errors in content moderation. It is also significant that certain regions where big tech companies have not invested sufficiently in localisation or staffing, and where public outcry by digital rights organisations is less likely to trigger platforms’ response than in the United States or Europe, may be more vulnerable to the risks of automated censorship. Consequently, users in smaller or less powerful countries may not receive the same protection against big tech’s decisions undermining their fundamental rights as their more influential counterparts.

Box 4: Digital dominance of the largest online platforms in numbers

<table>
<thead>
<tr>
<th>According to the UN’s Digital Economy Report 2019:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 40% of the world’s 20 largest companies (in terms of market capitalisation) have a platform-based business model;</td>
</tr>
<tr>
<td>• Global digital wealth is concentrated in the hands of a few online platforms based in the US and China. Both countries account for up to 90% of the market capitalisation value of the 70 largest digital platform companies in the world (US – 68%, China – 22%);</td>
</tr>
<tr>
<td>• Europe’s share is c.a. 4% and Africa and Latin America’s together is only c.a. 1%;</td>
</tr>
<tr>
<td>• 7 ‘super platforms’ – Microsoft, Apple, Amazon, Google and Facebook in the US, and Tencent and Alibaba in China – represent 2/3 of the total market value of the 70 largest platforms;</td>
</tr>
<tr>
<td>• Some digital platforms have grown to dominate key niches. Google has some 90% of the global market for internet searches, while Facebook accounts for 2/3 of the global social media market and is the top social media platform in more than 90% of the world’s economies. Amazon holds 1/3 market share of the world’s online retail activity and cloud services.</td>
</tr>
<tr>
<td>• In China, WeChat (owned by Tencent) has more than 1 billion active users. Its payment solution and Alipay (owned by Alibaba) have captured virtually 100% of the Chinese market for mobile payments. Meanwhile, Alibaba is estimated to have close to 60% of the Chinese e-commerce market.</td>
</tr>
<tr>
<td>• These companies keep consolidating their competitive positions, including by acquiring potential competitors and expanding into complementary products or services, lobbying in domestic and international policymaking circles, and establishing strategic partnerships.</td>
</tr>
</tbody>
</table>

---


Platforms’ arbitrariness and lack of transparency in content governance are also routinely used by actors seeking to spread harmful expression, such as racist speech, incitement to discrimination, or violence. Online platforms do not always adequately respond to this threat, as shown, for example, by the role that Facebook played in exacerbating violence against Muslims and the Rohingya ethnic minority in Myanmar in 2017–2018. In addition, online abuse of many marginalised groups is facilitated by social media companies allowing users to cover these actions behind automated accounts. It is also fuelled by their use of data-harvesting and profit-oriented business models, which amplify toxic content.

The ‘next generation’ measures which are used to curb free flow of online information presented in this section may seem more ‘subtle’ and limited in scope than, for example, blunt-force tactics, such as shutdowns. However, what distinguishes them from ‘older generation’ tools is that they are often less detectable by outside parties and more difficult to assign responsibility for, a feature which likely makes them more effective.

### 2.5. Transnational dimensions of digital repression

Another very serious challenge, which has emerged in recent years, is proliferation of a so-called ‘transnational digital repression’. It has become apparent that regimes with restrictive domestic internet policies and advanced digital surveillance have been increasingly ‘extending’ these practices beyond their borders to affect targets living in foreign countries. In particular, development of new information and communication technologies has facilitated targeting regime opponents living in the diaspora. Even though transnational repression has been a long-standing problem for diasporas with ties to authoritarian sending-states, digital tools have allowed such governments to control, silence, and punish dissident across borders with greater scope, speed and at reduced cost, transcending traditional barriers, such as territorial jurisdiction and physical distance. The rise of new digital and information technologies, services and tools, as well as playing a central role in the targeting of activists based abroad, has enabled more effective identification and tracking of dissident networks, including monitoring of their activities, hacking of their social media accounts and websites, the planting of malware, phishing for confidential information, online harassment, and disinformation campaigns. Not only has this facilitated long distance forms of repression targeted directly at those residing abroad, but also ‘coercion-by-proxy’ – exerting control and inducing fear via relatives still in...

---

124 UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, op. cit., par. 24-25.
125 Deibert, R., op. cit., p. 65.
126 Defined as activities undertaken by states ‘seeking to exert pressure - using digital tools - on citizens living abroad in order to constrain, limit, or eliminate political or social action that threatens regime stability or social and cultural norms within the country. See: Al-Jizawi, N., Anstis, S., Chan, S., Senft, A. and Deibert, R.J., ‘Annotated Bibliography. Transnational Digital Repression’, Citizen Lab, University of Toronto, 2020.
128 It has been established that ‘for diaspora activists engaging for political change in their country of origin, digital technologies are key to communicate with contacts at home, maintain professional relations, and advocate against rights violations’. This activity makes them particularly ‘exposed to monitoring and surveillance from regime authorities’. See Michaelsen, M., ibidem.
the country. This is because new methods of digital surveillance make it easier for authoritarian states to identify ties between activists living in diaspora and family members or acquaintances ‘back home’\textsuperscript{129}. It has also been established that, in response to activists’ attempts to protect themselves using methods like encryption, the authoritarian regimes have been applying even more aggressive measures of targeted surveillance (in addition to still in place ‘traditional’ mechanisms of repression, such as arrests or physical harassment)\textsuperscript{130}.

The most prominent examples of digital transnational repression are the deployment of cyberespionage campaigns by China against Tibetan diaspora or pro-democracy groups in Hong Kong\textsuperscript{131}, Saudi Arabia’s deployment of spyware on the mobile devices of Saudi political activists living in Canada or the United Kingdom\textsuperscript{132}, and disruption operations of media and opposition websites based abroad, including defacement and DDoS campaigns by hackers affiliated with Syrian or Iranian regimes\textsuperscript{133}. Digital transnational repression practices have also affected targets living in EU countries. It was revealed, for example, that Turkey, known for its current widespread repressive campaign against suspected opponents abroad (including, in particular, mobility controls, detentions and illegal renditions), developed a smartphone application to be used for reporting potential members of the Gülen movement\textsuperscript{134} to the authorities in Ankara from among the Turkish diaspora in Germany\textsuperscript{135}. At the same time, digital threats against activists living abroad have been linked to several other countries across the world in recent years (one of the studies indicates, for example, that the Bahrain, Burma, Eritrea, Ethiopia, Kazakhstan, Rwanda, United Arab Emirates, Uzbekistan, and Vietnam governments are among those implicit in this)\textsuperscript{136}. Documented negative effects of such transnational repressive actions on diaspora activism include increased self-censorship among human rights defenders that may be targeted by those practices, more careful management (or even breaking up) of their ties to the home country and higher risk of mental stress and burnout. Still, further research is required to understand how transnational digital repressions affect social and political lives of their target groups\textsuperscript{137}.

Other examples illustrating an expansion of regime control outside of the nation state, not necessarily targeted at political exiles and diaspora communities, include using the private sector for this purpose. One tactic is to exploit domestic companies functioning on international markets and their technological products to export existing surveillance and censorship practices abroad. There is evidence, for example, that communications on Chinese WeChat, the most popular social media platform in China and third in the world, conducted entirely between non-China-registered accounts, have been ‘subject to pervasive content surveillance that was previously thought to be exclusively


\textsuperscript{130} Michaelsen, M., op. cit.


\textsuperscript{133} Al-Jizawi, N., et. al, op. cit.

\textsuperscript{134} A movement related to a religious leader Fethullah Gülen, which the Turkish government blames for the coup attempt in 2016.


\textsuperscript{136} Al-Jizawi, N., et. al, op. cit.

\textsuperscript{137} Michaelsen, M., op. cit.
reserved for China-registered accounts. Another strategy engaging the private sector involves imposing pressure on globalised tech companies to comply with governments’ regulations and suppress the flow of unwelcome information beyond national borders (which, to some extent, may also be facilitated by non-transparent content moderation policies and practices of online platforms). Zoom Video Communications, for example, a US-based video-tech company, recently admitted that, following the Chinese government’s demands, it suspended a number of user accounts and ended meetings on its platform linked to the anniversary of China’s Tiananmen Square crackdown.

Last but not least, digital surveillance in a number of abusive regimes is facilitated by the import of surveillance equipment from other countries, often marketed as tools to assist governments in lawful investigations into crime and terrorism. While certain regimes rely on their own digital surveillance tools, other states (which often do not have the same capacity to develop their own technology), invest in ‘off-the-shelf’ solutions that are acquired from private sector companies specialising in targeted cyber-espionage. Some of these are based in western countries (including EU Member States), such as the United States, the United Kingdom, Germany, Netherlands, France, Sweden and Israel, and have significantly proliferated globally in the recent years. At the same time, China’s role in the export of surveillance technologies has significantly increased, offering more affordable packages potentially attractive to governments that want to develop their surveillance model, while still importing sophisticated biometric surveillance tools from Europe. A prominent example of a company exporting its spyware products to a number of countries with dubious human rights records is the Israel-based NSO Group, provider of a Pegasus spyware system, which is further elaborated on in section 2.6 below.

Of note, a targeted surveillance technology that is closely related to spyware but has some distinctions is digital forensics or mobile phone extraction. Similar to spyware, this tactic involves extracting, analysing, and presenting data and information found on mobile devices and computer systems. Rather than use software to “hack” into a device, digital forensics relies on a physical connection in


139 Governments may take advantage of those opaque mechanisms to restrict access to politically inconvenient content. Instead of following the required procedures (e.g. getting a court order), they can ‘choose the easy way’ and use the self-regulation mechanisms of the online platforms to achieve the same result without the procedural restrictions.


which to obtain data. Major commercial players include Cellebrite, Oxygen Forensic Detective, and MSAB.\textsuperscript{144}

### 2.6. Pegasus and equivalent surveillance spyware

#### 2.6.1. The emergence of targeted surveillance and its models of operation

In the recent years, the issue of surveillance spyware has taken on increased attention, mostly due to revelations related to the surveillance and spying of persons, including Prime Ministers and Members of Parliament, journalists, NGOs and human rights activists. “Pegasus Project”, a global investigation initiative revealed that governments have expanded their use of digital surveillance techniques, included “military-grade” software acquired from the Israeli firm NSO Group, to hack into smartphones, track citizen communications, and acquire incriminating information, sometimes in preparation for extra-judicial killings\textsuperscript{145}. Spyware belongs to a category of tools classified as intrusion software, which are designed to manipulate software, computer systems, mobile devices, or networks in order to access and extract data and information\textsuperscript{146}. Unlike other forms of surveillance, such as mass surveillance, which governments deploy towards a wider range of individuals or groups in an undifferentiated manner, targeted surveillance operations involve specific deployments of malware or spyware to collect information.

Experts classify targeted surveillance operations into three models: national in-house operations or advanced persistent threat (APT), repurposed crimeware or ‘hackers in the middle’, and commercial spyware\textsuperscript{147}. APT operations, an integral component of the first model, entails a ‘sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time’\textsuperscript{148}. APT attacks are carefully planned to penetrate specific organisations and to evade existing security measures. APT operations are largely designed and executed by high-capacity states, such as the National Security Agency’s ‘tailored access operations’ group, Israel’s Unit 8200, or equivalent Chinese or Russian actors which receive direct or tacit government support\textsuperscript{149}.

The second category, repurposed crimeware or ‘hackers-for-hire’ involve outsourcing targeted intrusion attacks to for-profit hacker collectives, smaller spyware vendors, or domestic contractors. In Syria, for example, the Citizen Lab documented how basic Remote Access Trojans (RATs), which are programs that circulate among ‘hobbyists and criminals’, were subsequently deployed in Syria for political reasons linked to the country’s civil war. This approach ‘blurs the worlds of cybercrime and espionage, and is forged out of necessity and, to some degree, a kind of “do-it-yourself” mentality’\textsuperscript{150}. Many repressive governments (as well as criminal syndicates) are turning to hacker-for-hire groups that can provide relatively inexpensive malware that deliver good enough results with few questions asked in return.

\textsuperscript{144} Privacy International (2019), A technical look at Phone Extraction
\textsuperscript{145} The Washington Post (2021), Takeaways from the Pegasus Project
\textsuperscript{146} Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public Documents, Volume II, List of Dual-Use Goods and Technologies and Munitions List
\textsuperscript{147} Citizen Lab, University of Toronto (2014), Communities @ Risk: Targeted Digital Threats Against Civil Society
\textsuperscript{148} Crowdstrike (2022), Advanced Persistent Threat
\textsuperscript{149} Der Spiegel (2013), Documents Reveal Top NSA Hacking Unit, Haaretz (2021), An Elite Israeli Intelligence Unit’s Soldiers Are Sworn to Secrecy – but Tell All on LinkedIn
\textsuperscript{150} Citizen Lab, University of Toronto (2014), Communities @ Risk: Targeted Digital Threats Against Civil Society
The third category involves commercial spyware provisioned from firms that sell products and services to governments, law enforcement, and intelligence agencies. NSO Group’s Pegasus program falls into this group. These products are more sophisticated and come at a higher cost than the crimeware packages in the second category, but they do not require actors to have an in-house capacity to develop or operate targeted cyber attacks. Instead, governments can purchase these capabilities directly from companies. The products’ high cost and claim by spyware vendors that sales are limited to government clients, makes this primarily a state-based option. Vendors such as NSO Group, FinFisher, and Cellebrite are major players in this sector and have attracted a high degree of controversy.

2.6.2. Commercial spyware surveillance chain

When it comes to implementing intrusion attacks, some researchers classify operations into three phases making up the ‘surveillance chain’: reconnaissance, engagement, and exploitation\(^\text{151}\). The reconnaissance phase is the least visible to targets and involves profiling targets and pulling information about them from online records (often marketed as ‘web intelligence services’). The goal is to obtain operationally relevant information that can facilitate subsequent attacks.

The engagement phase aims to establish contact with targets to ‘build trust, solicit information, and trick them into clicking on links or downloading files’\(^\text{152}\). Spyware operators have relied on methods such as social engineering (psycho-logical manipulation to trick users into revealing information in order to compromise their devices or online accounts) or spear phishing (malicious files or links delivered by email that are intended to bait targets into installing spyware to compromise their devices or accounts) to gain access to confidential communications, records, and data.

The exploitation phase of the surveillance chain entails the actual delivery of malicious payload. Operators can custom-build their own exploits or can acquire malicious tools from other vendors to deliver the malware. The level of sophistication varies. NSO Group, for example, helped pioneer the rise of ‘zero-click’ exploits, where attackers are able to access a user’s smartphone simply by uploading phone numbers or email addresses. As Bloomberg’s Ryan Gallagher explains, zero-click techniques ‘exploit a series of security flaws in operating systems — such as Apple Inc.’s iOS or Google’s Android — to breach a device without having to dupe their victim into taking any action’\(^\text{153}\). Once the intruders have gained access, they can do a myriad of things: install malware that can steal data, snoop on phone calls, or track the user’s location. While NSO Group is the most well-known vendor which has developed zero-click exploits, other companies also offer these tools.

Regulators have begun to take notice. On November 2021, for example, the U.S. government added Candiru, along with NSO Group, Russia’s Positive Technologies and Singapore’s Computer Security Initiative Consultancy to the Commerce Department’s Entity List, based on evidence that these firms provided spyware used to ‘maliciously target’ government officials, journalists, activists, academics, diplomats, and businesspeople\(^\text{154}\). The consequences for landing on the Entity List are severe – U.S. firms are prohibited from exporting, re-exporting or transferring (in-country) to the companies added.

---

\(^\text{151}\) Meta (2021), Threat Report on the Surveillance-for-Hire Industry
\(^\text{152}\) Meta (2021), Threat Report on the Surveillance-for-Hire Industry
\(^\text{153}\) Bloomberg (2022), Zero-Click’ Hacks Are Growing In Popularity. There’s Practically No Way To Stop Them
\(^\text{154}\) U.S. Department of Commerce (2021), Commerce Adds NSO Group And Other Foreign Companies Entity List
to the list. As a result, NSO Group has been hit with financial problems and announced the resignation of its CEO, Shalev Hulio, on September 22, 2022, along with the laying off of over 100 employees.\(^{155}\)

While commercial spyware vendors are facing a greater degree of scrutiny from democratic governments than they have in the past, there has been a concurrent rise in a distinct, but related problem: the increase of open-source and commercially available malware, which has made it easier for groups to mount attacks. Facebook’s 2022 quarter adversarial threat report describes the shifting trend, noting that APT groups are choosing to rely on ‘openly available malicious tools, including open-source malware, rather than invest in developing or buying sophisticated offensive capabilities’.\(^{156}\)

While some groups are opting for more advanced malware that incorporates exploits, a growing number of operations are using ‘basic low-cost tools that require less technical expertise to deploy yet yield results for the attackers nonetheless’.\(^{157}\) This shift is serving to democratize access to hacking and surveillance capabilities due to a lowered ‘barrier to entry’. For example, the report documents a group of hackers from Pakistan known as APT36, which targeted government and military officials, as well as activists. Their goal was to get individuals to inadvertently install malware, which they were able to download for free from Github.\(^{158}\)

Another implication is that groups relying on low-cost tools are able to hide in the ‘noise’ and acquire plausible deniability about which organization was actually responsible for initiating the attack. As Casey Newton writes, ‘malware created by state actors often carries tell-tale signs of who developed it in its code; when everyone is using the same code, though, platforms lose an important signal...If a bunch of different threat actors are throwing the same malware all over the internet, it makes it harder for analysts to pull together exactly who is behind it’.\(^{159}\) This helps explain why in certain situations actors may prefer to rely on commonly sourced code for intrusion attacks rather than commercial spyware.

2.6.3. Global proliferation of commercial spyware

In the recent years, NSO Group and its Pegasus spyware tool received significant public attention. The Citizen Lab first started investigating Pegasus in 2016 and generated several reports, beginning in 2018, tracking Pegasus spyware to operations in at least 45 countries linked to human rights violations targeting civil society.\(^{160}\) In 2021, the Citizen Lab joined with Amnesty International, Forbidden Stories, and 17 media outlets for a combined investigation about government use of Pegasus worldwide to spy on journalists, political opposition members, civil society, and government officials. The investigation identified over 50,000 numbers linked to more than 1,000 people who were targets of Pegasus across over 50 countries, including ‘several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials — including cabinet ministers, diplomats, and military and security officers’.\(^{161}\) At least 10 prime ministers, three presidents, and one king were also found on Pegasus target lists. What has been somewhat lost in the clamour against NSO Group is the fact that a multitude of other commercial spyware vendors

---

\(^{155}\) The Guardian (2022), CEO of Israeli Pegasus spyware firm NSO to step down, Engadget (2022), NSO Group CEO Shalev Hulio Stepping Down

\(^{156}\) Meta (2022), Meta’s Adversarial Threat Report, Second Quarter 2022

\(^{157}\) Meta (2022), Meta’s Adversarial Threat Report, Second Quarter 2022

\(^{158}\) APT36 downloaded a free tool from Github known as XploitSPY, reportedly developed “by a group of self-reported ethical hackers in India.” Why Microsoft-owned Github would host code that could be used to target government officials and activists remains unclear, Platformer (2022), Three Wild Stories From Facebook’s Counter Espionage Team

\(^{159}\) Platformer (2022), Three Wild Stories From Facebook’s Counter Espionage Team

\(^{160}\) Citizen Lab, University of Toronto (2018), Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries

\(^{161}\) The Washington Post (2022), Private Israeli Spyware Used to Hack Cellphones of Journalists and Activists Worldwide
have been involved in similar sales that have resulted in significant human rights harms. Many
government clients, such as Myanmar’s junta, leave little ambiguity when it comes to their methods of
use. Yet, despite a growing international outcry, commercial spyware sales persist. The following case
studies offer illustrative examples of global spyware use and relevant trends.

Box 5: Use of Pegasus in Thailand

Thailand provides an illuminating example regarding how Pegasus facilitates non-democratic
objectives. A 2022 Citizen Lab investigation revealed that the Thai government contracted with
Israel-based NSO Group to obtain Pegasus exploits that were subsequently used against at
least 30 victims based in Thai civil society groups. Targeted individuals included activists,
lawyers, academics, and NGO workers. The Thai government has a history of using spyware to
keep tabs on opposition figures. Previous reports indicate that multiple Thai agencies had
contracted with the firm Circles (subsequently acquired by NSO Group’s holding company Francisco
Partners) and Hacking Team to surveil political opponents. In the latest instance involving Pegasus,
the Thai regime faced escalating protests from pro-democracy activists in the October 2020 to
November 2021 timeframe. In November, Apple began sending notifications to iPhone users
disclosing they were potential victims of an attack. This triggered the Citizen Lab to initiate an
investigation, along with Thai organizations iLaw and DigitalReach. They found evidence that “two
zero-click exploits” linked to NSO Group (Kismet and Forcedentry exploits) were used against the
examined phones. There was no evidence of the use of one-click exploits. In this case, the forensic
evidence does not directly point to a particular Pegasus operator, but ‘numerous elements of the
case, when taken together, provide circumstantial evidence suggesting one or more Thai
government Pegasus operators is responsible for the operation’.

Among the spyware targets were prominent opposition and civil society figures who the
government had repeatedly detained, arrested, or imprisoned. Spyware victims include four
members of a prominent youth movement – United Front of Thammasat and Demonstration;
a leading human rights lawyer and protest leader, Arnon Nampa; the Thai digital rights
organization – iLaw (which collaborated with Citizen Lab on the spyware investigation); as
well as Thai actor Inthira Charoenpura, who financially supports protestors. iLaw researchers
speculate that Thai authorities were motivated to use Pegasus for three purposes: ‘to monitor the
online activities of dissidents; to monitor the protests; and to seek information about the funding
sources for the protests’. It is also likely that some of the private communications picked up by the
authorities were subsequently used in lèse-majesté prosecutions (a law which criminalizes insults
and defamations against the Thai royal family and results in long prison sentences) and cyber law
prosecutions.

There is a clear linkage between the Thai government’s repressive objectives – suppress pro-
democracy movements that threaten the regime – and its acquisition of spyware to target
regime challengers. As a result of the Pegasus deployment, Thailand’s government has been
able to impose more stringent controls on information and has increased its capacity to
silence dissent, particularly on the internet. The Thai government has a history of using spyware

162 Citizen Lab, University of Toronto (2022), Geckospy: Pegasus Spyware Used Against Thailands pro-Democracy Movement
163 Citizen Lab, University of Toronto (2022), Geckospy: Pegasus Spyware Used Against Thailands pro-Democracy Movement
164 Citizen Lab, University of Toronto (2022), Geckospy: Pegasus Spyware Used Against Thailands pro-Democracy Movement
165 iLaw Freedom (2022), Parasite that Smiles: Pegasus Spyware Targeting Dissidents in Thailand
to facilitate crackdowns on political opponents – there is widespread evidence of human rights violations linked to surveillance technology both in Thailand and in other countries where Pegasus has been deployed.

2.6.4. Emergence of Cytrox Predator

While Pegasus has received substantial attention, other spyware programs have generated harms as well – such as Predator software, developed by the firm Cytrox. Cytrox has an ambiguous origin. It appears to have begun as a North Macedonian start-up. It currently is registered in Israel and Hungary. Cytrox was apparently “rescued” by Tal Dilian, a former Israeli Defense Forces officer who earlier founded the spyware firm Circles and who currently operates Intellexa, which comprises a consortium of spyware companies including Nexa Technologies, WiSpear/Passitora, Cytrox, and Senpai.

According to current reporting, Predator uses one-click infections (requiring a user to click on a link to activate the malware). In infected iPhones, for example, the iOS loader will install a Predator configuration file and download an iOS shortcuts automation from the Predator server to ensure persistence. iOS automation is triggered when certain apps are opened, including Apple apps (camera, mail, maps, safari) and third-party apps (Twitter, Instagram, Facebook Messenger, LinkedIn, Skype, Snapchat, Viber, Wire, TikTok, Line, OpenVPN, WhatsApp, Signal, and Telegram). In basic terms, Predator spyware ‘allows operators to monitor every aspect of a target’s phone, including calls, messages, photos and video’. Predator has received far less attention than Pegasus, but it is starting to gain notice. In the summer of 2022, for instance, researchers from the Citizen Lab and Google revealed that Greece’s national intelligence services had likely purchased Predator software to spy on Nikos Androulakis, leader of the country’s opposition.

Greece was not the only country using Predator software in a questionable manner. Researchers conclude that Predator is likely being used by government-backed operators in Egypt, Armenia, Madagascar, Côte d’Ivoire, Serbia, Spain, and Indonesia. In a December 2021 report, the Citizen Lab specifically traced Predator spyware to the hacking of exiled Egyptian politician Ayman Nour’s phone, as well as the hacking of an exiled Egyptian journalist hosting a popular news program. What was particularly eye-opening about this circumstance, is that Citizen Lab researchers found that Nour’s phone was hacked using both Predator and Pegasus software, likely coming from two separate Egyptian government agencies. Phone logs suggest that on several occasions, Pegasus and Predator were ‘running simultaneously’ on Nour’s phone. This leads to several chilling conclusions. It illustrates the extent to which the commercial spyware industry is far from reliant on a single company, even if that company is responsible for selling more advanced zero-click products. In Saudi Arabia, for example, reports indicate that NSO Group cut off the Saudi government as a client ‘amid accusations that its hacking tools were being misused to abet heinous crimes’. Subsequently, the Citizen Lab began matching Cytrox Predator ‘fingerprints’ to an IP address in Saudi Arabia, entailing that Saudi Arabia likely substituted Predator for Pegasus spyware when it was dropped by NSO. The interspersed

---

166 Forbes (2019), A Multimillionaire Surveillance Dealer Steps Out Of The Shadows . . . And His $9 Million WhatsApp Hacking Van

167 European Parliament, “Greece’s Predatorgate The latest chapter in Europe’s spyware scandal?”

168 Google (2022), Protecting Android users from 0-Day attacks; Bloomberg (2022), Greece, EU Accused of Probing Spy Scandal Only in ‘Superficial Way’

169 Citizen Lab (2021), Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware

170 Citizen Lab (2021), Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware

171 New York Times (2021), Israeli Companies Aided Saudi Spying Despite Khashoggi killing
use of Pegasus and Predator spyware ‘underscores that the practice of hacking civil society transcends any specific mercenary spyware company’\(^{172}\). As along as authoritarian governments are able to acquire sophisticated spyware, this pattern will continue.

### 2.6.5. Cellebrite’s data extraction technology

Another prominent Israeli surveillance vendor implicated in selling sophisticated snooping technology to an array of authoritarian governments is Cellebrite. Unlike NSO Group, Cellebrite has developed a tool – the Universal Forensic Extraction Device (UFED) – which requires physical access to a target’s phone, but which then allows operators to break into password-protected mobile phones when connected to an investigator’s desktop computer\(^{173}\). Cellebrite sells these devices in a variety of forms, including a field-based version, which is approximately the size of an iPad. The company markets itself as a ‘defender of human rights’ and has trumpeted its withdrawal from markets such as Bangladesh, Belarus, China, Hong Kong, Russia, and Venezuela\(^{174}\). But there are several problems with this claim. In the case of China, for example, even after Cellebrite claimed to exit the market and deregister its Chinese subsidiary in early 2021, third-party resellers continue to peddle Cellebrite technology to police departments and security agents. As Mara Hvistendahl writes in *The Intercept*: ‘In one case, a reseller reported delivering the Israeli company’s software to border guards in Tibet and demonstrating how it could be used to search people’s WeChat accounts’\(^{175}\). Therefore, unless Cellebrite is willing to take active steps to stem the reach of its products in deactivated markets and to make obsolete the software needed to run on the UFED devices, its words carry little weight. (Also of note: the likely main reason Cellebrite exited the above markets was due to a series of investigative reports carried out by Israeli human rights lawyer Eitay Mack regarding Cellebrite’s sales to regimes such as Saudi Arabia and Belarus\(^{176}\).)

**Circumstances in Bangladesh illuminate the troubling use of technology from Israel-based Cellebrite.** In Bangladesh, the Rapid Action Battalion (RAB), a notorious paramilitary unit accused of carrying out extra-judicial killings, torture, and disappearances, has been linked to the purchase of Cellebrite’s UFED devices. Reports indicate that a May 2021 government budget authorized the RAB to acquire ‘an additional Cellebrite system’\(^{177}\). Cellebrite technology had reportedly reached the RAB unit through the firm’s representatives in Singapore. As part of the support package, Cellebrite provided training to RAB officers in Singapore in 2018 and 2019. In the same year (2018) in which the RAB first procured Cellebrite’s data extraction devices, the unit was allegedly responsible for committing 466 extrajudicial killings (a threefold increase from the prior year)\(^{178}\). Surveillance technologies figure prominently in the government’s crackdown on dissent. Human Rights Watch notes that victims of state-sponsored abductions report the use of surveillance, including ‘interception of telecommunications and tracking social media’ in the lead up to kidnappings\(^{179}\). **Authorities routinely deploy surveillance measures to ‘crack down on any criticism of the government,**

---

\(^{172}\) Citizen Lab (2021), [Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware](https://www.citizenlab.org/en/2021/06/pegasus-vs-predator-dissident-s-doubly-infected-iphone-reveals-cytrox-mercenary-spyware)

\(^{173}\) The Intercept (2021), [Chinese Police Kept Buying Cellebrite Phone Crackers After Company Said It Ended Sales](https://theintercept.com/2021/09/15/chinese-police-kept-buying-cellebrite-phone-crackers-after-company-said-it-ended-sales/)

\(^{174}\) US Securities and Exchange Commission, June 29, 2021, Registration No. 333-256177, Cellebrite DI Ltd.

\(^{175}\) The Intercept (2021), [Chinese Police Kept Buying Cellebrite Phone Crackers After Company Said It Ended Sales](https://theintercept.com/2021/09/15/chinese-police-kept-buying-cellebrite-phone-crackers-after-company-said-it-ended-sales/)


through arrests as well as enforced disappearances"¹⁸⁰. During the Covid-19 pandemic, the government expanded its surveillance program by creating a unit under RAB to identify Covid-19 ‘rumours’ leading to the enforced disappearance and arrest of individuals criticizing the government’s public health response. Prominent arrested individuals include: the cartoonist Ahmed Kabir Kishore; Mushtaq Ahmed, a writer and activist; Didarul Bhuiyan, an activist; and Minhaz Mannan Emon, head of the Dhaka Stock Exchange. All were arrested under the Digital Security Act for publishing material critical of the government’s handling of the Covid-19 pandemic, which “had been discovered by the RAB-3 cyber team, the surveillance unit created to weed out any Covid-19 ‘rumours’”¹⁸¹.

Despite a widespread pattern of abuse associated both with the RAB and other security forces in the country, Cellebrite had few qualms providing invasive technology to a unit known for being a “death squad” until its actions were exposed by Mack¹⁸².

2.6.6. Europe as a “nexus” for commercial spyware

Notwithstanding growing concerns in Europe about commercial spyware proliferation, European companies are responsible for selling tools worldwide linked to an array of human rights abuses. Two notorious spyware firms – FinFisher and Hacking Team – were based in Germany and Italy, respectively. Hacking Team’s RCS software allowed Ethiopian government agents to target US-based journalists based out of the Ethiopian Satellite Television Service¹⁸³. The software was also used against Moroccan media outlet Mamfakin and was deployed to snoop on UAE human rights activist Ahmed Mansoor¹⁸⁴. Similarly, Ethiopian operators used FinFisher’s FinSpy malware to target dissidents, while Bahrain’s government deployed FinSpy to track and monitor law firms, journalists, activists, and opposition politicians¹⁸⁵.

The use of FinFisher’s software by Bahraini authorities is instructive. Leaked documents from 2014 show that Bahrain’s government had procured FinSpy malware from German company FinFisher, a subsidiary of UK-based Gamma International (Bahrain’s Ministry of Interior has been linked to the procurement of malware)¹⁸⁶. Like other types of malicious software, FinSpy allows an outside user to gain remote access to computers and mobile devices of targeted users. Once installed, FinSpy software enables the operator to collect data, search files, read communications, and impersonate the target online. Dating back to 2012, Bahrain targeted large numbers of activists and human rights defenders with FinFisher’s products – both at home and overseas. The leaked documents indicate that FinFisher helped Bahrain install spyware on at least 77 computers¹⁸⁷. In one documented example, the computer of prominent Bahraini lawyer Mohamed Altajer, ‘was hacked on the same day as a blackmail attempt against him’¹⁸⁸. The lawyer had received a CD instructing him to stop defending activists, ‘otherwise a video included on the CD would be publicized’¹⁸⁹. The CD contained a private

¹⁸² Haaretz (2021), Israeli Cellebrite Sold Spy-tech to Bangladesh ‘Death Squad’
¹⁸³ Citizen Lab (2015), Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware
¹⁸⁴ Citizen Lab (2015), Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware; Citizen Lab (2017), Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware
¹⁸⁵ Citizen Lab (2015), Pay No Attention to the Server Behind the Proxy: Mapping FinFisher’s Continuing Proliferation
¹⁸⁶ Privacy International (2014), Six things we know from the latest FinFisher documents
¹⁸⁷ The Intercept (2014), Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters
¹⁸⁸ Citizen Lab (2021), From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits
¹⁸⁹ Citizen Lab (2021), From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits
hacked video of Altajer engaged in intimate relations with his wife, ‘recorded from a hidden camera installed in the ceiling of his house’\textsuperscript{190}. The video became public after Altajer participated in a human rights conference sponsored by the UN. He described the posting of the video as ‘the most devastating day of my life’\textsuperscript{191}. While FinFisher and Hacking Team are now bankrupt, in part due to a proliferation of investigations and lawsuits (as well as an infamous “hack” of Hacking Team, which leaked its client list), other firms in Europe have taken their place\textsuperscript{192}.

One such entity is a small Italian company named Tykelab, owned by RCS Lab. Tykelab has exploited unfixed vulnerabilities in global phone networks, enabling clients to track individuals’ locations and intercept calls in countries such as Kazakhstan, Iraq and Italy. The firm has developed a powerful hacking tool, Hermit, able to ‘remotely activate microphones, record calls, access messages, call logs, contact lists, photos and other sensitive phone data’\textsuperscript{193}. According to a recent investigation from Lighthouse Reports and Google TAG, Tykelab’s surveillance tools have been used to target individuals around the world, including in Costa Rica, Iraq, Kazakhstan, Malaysia, Mali, Nicaragua, Pakistan, as well as in Greece, Italy, Macedonia, and Portugal\textsuperscript{194}.

Another company, Sweden’s MSAB (known as the ‘European equivalent of Cellebrite’) has developed technology to break mobile phone encryption and extract ‘call, contact, GPS, and other records, as well as messages sent and received via SMS, WhatsApp, Signal, and other apps’\textsuperscript{195}. MSAB’s products also allow clients to extract passwords and login tokens from mobile devices so they can break into users’ online services, such as Google, Facebook, and cloud storage.

MSAB has a particularly troubling record in Myanmar. The firm has acknowledged that it sold its forensic tools to the Myanmar police in 2019, just two years after security forces committed atrocities in Rohingya. More recently, in 2021, leaked documents indicate that MSAB intended to sell phone extraction technology to Myanmar’s Bureau of Special Investigations (BSI) via a third-party distributor. BSI is the intelligence arm of the Ministry of Home Affairs, which manages domestic security and is controlled by the military. While MSAB called off the deal following the February 2021 coup, MSAB’s earlier products remain in the hands of Myanmar’s security forces\textsuperscript{196}. The human rights impact of MSAB’s tools is significant. Scores of imprisoned activists have had their mobile devices scanned for incriminating information using MSAB tools. For example, reporting from The Intercept describes the arrest of a Burmese student named “Myat” (name changed to protect his identity) in March 2021\textsuperscript{197}. Officials dragged and beat him until he lost consciousness. When he awoke in a police car, authorities forced him to unlock his smartphone, which they subsequently confiscated (and presumably scanned for communications and contacts). Authorities moved him to a military compound in Shwepyithar Township – used by the junta to detain protesters, journalists, and others. The police eventually released Myat and returned his phone, but he lacks any means to

\textsuperscript{190} Citizen Lab (2021), From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits
\textsuperscript{191} The Intercept (2014), Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters
\textsuperscript{192} Wired (2015), Hacking Team’s oppressive regimes customer list revealed in hack
\textsuperscript{193} Lighthouse Reports (2022), Revealing Europe’s NSO
\textsuperscript{194} Google (2022), Spyware vendor targets users in Italy and Kazakhstan; Lighthouse Reports (2022), Revealing Europe’s NSO
\textsuperscript{195} The Intercept (2021), Tools For Repression In Myanmar Expose Gap Between Eu Tech Investment And Regulation
\textsuperscript{196} The Intercept (2021), Tools For Repression In Myanmar Expose Gap Between Eu Tech Investment And Regulation
\textsuperscript{197} The Intercept (2021), Tools For Repression In Myanmar Expose Gap Between Eu Tech Investment And Regulation
determine which parts of his phone were accessed during his four-day imprisonment or whether authorities are still monitoring his device\textsuperscript{198}.

Other examples of European firms peddling spyware abound. For instance, in July 2022, operators used spyware from Austrian firm DSIRF to hack into law firms, banks, and consultancy firms in Austria, Panama, and the UK. According to Microsoft researchers, DSIRF’s ‘subzero’ tool used zero-day exploits to access confidential information, such as passwords and other credentials\textsuperscript{199}.

What is telling about these incidents is the extent to which the spyware industry extends beyond NSO Group. As Etienne Maynier, from Amnesty International’s Security Lab, notes: ‘Even if NSO Group closes tomorrow because of all the problems they face today, the situation will be the same if there is no change in the regulation. The problem is not one bad company. It’s really the legal structure that makes these companies take these decisions’\textsuperscript{200}. Given the prominence of European firms in the international commercial spyware industry, it is incumbent that European regulators take a harder look at lax regulations which continue to allow companies to propagate intrusion tools to bad actors.

Box 6: Global spread of spyware – updated indicators

Since December 2020, Steven Feldstein has collected data regarding the global spread and distribution of commercial spyware technology, focusing on which governments show evidence of procuring and employing intrusion technology and which commercial firms are involved. The most recent version, dated December 2022, shows that at least 74 countries worldwide, including a mix of authoritarian states and democracies, have purchased commercial spyware or digital forensics technology from firms such as NSO Group, Cellebrite, Hacking Team, FinFisher, Candiru, and many others\textsuperscript{201}. This figure represents a considerable increase from the prior version of the dataset released on December 22, 2020, which listed 64 countries procuring commercial spyware\textsuperscript{202}. Figure 1 depicts the geographic distribution of countries deploying commercial spyware and digital forensics technology.

\textsuperscript{198} The Intercept (2021), Tools For Repression In Myanmar Expose Gap Between Eu Tech Investment And Regulation
\textsuperscript{199} Microsoft (2022), Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits
\textsuperscript{200} Wired (2022), Spyware Scandals Are Ripping Through Europe
\textsuperscript{201} Mendeley Data (2020), Steven Feldstein, “Commercial Spyware Global Inventory”
\textsuperscript{202} For analytic commentary describing the previous global commercial spyware inventory findings, see Carnegie Endowment for International Peace (2021), Steven Feldstein, “Governments Are Using Spyware on Citizens. Can They Be Stopped?”; Mendeley Data (2020), Steven Feldstein, “Commercial Spyware Global Inventory”
2.6.7. Policy discussion around Pegasus and equivalent surveillance spyware

Given the documented harms associated with spyware, it is fair to ask why democracies have failed to regulate or ban the commercial use of spyware. Three general reasons explain the reluctance of many governments to rein in the global spyware industry.

First, many governments have a geopolitical interest in sustaining commercial spyware firms. While spyware can lead to significant harms through the unlawful targeting of citizens, they also provide geo-strategic benefits for countries that rely on intelligence and spy craft to advance their interests. Even for highly capable countries like the United States or United Kingdom, which possess powerful in-house competencies, it can be advantageous to rely from time to time on outside firms to conduct cyber attacks or hacking operations against adversaries. Commercial spyware firms can offer plausible deniability to sponsoring governments and also possess the necessary capacity to carry out sensitive missions.

Second, some law enforcement and intelligence agencies rely on commercial spyware to confront legitimate threats that endanger national security or public order. While certain governments, particularly authoritarian regimes, exploit national security carveouts for illegitimate uses, specific circumstances may warrant using these tools, such as for apprehending dangerous suspects or preventing imminent harm to civilians. It is conceivable that putting in place enforceable legal frameworks premised on necessity, proportionality, and lawfulness could alleviate some of the abuses associated with the industry, although most experts maintain that use of spyware should be limited to the most serious crimes or graver threats to national security, and even then, governments should only rely on these tools as a last resort, after less intrusive measures have been exhausted.

---

203 The most recent version of the global spyware inventory, including countries, commercial spyware and digital forensics vendors, and event descriptions can be accessed publicly at: https://data.mendeley.com/datasets/csvhpkt8tm/7

204 OHCHR (2022), Spyware and surveillance: Threats to privacy and human rights growing, UN report warns
Third, for exporting countries, the spyware industry can be a lucrative source of revenue and a lever for diplomatic influence. Israel is a good case in point. Many Israeli firms enjoy a close relationship to Israel’s intelligence agency, particularly its cybersecurity division, Unit 8200. A 2018 study cited in Haaretz found that 80 percent of the 2,300 people who founded Israel’s 700 cybersecurity companies were former employees of the Israeli Defense Forces’ intelligence units. These companies have sold surveillance technology throughout the world to governments such as Botswana, Saudi Arabia, Mexico, Ethiopia, Kazakhstan, Nigeria, and Indonesia. The industry’s collective sales are estimated to be at least $1 billion annually. When the United States placed NSO Group on its Entity List, effectively putting the company on life support, the reaction from Israel’s government was fierce. Israeli diplomats were said to be orchestrating a diplomatic ‘campaign’ to remove sanctions against NSO as well as Candiru, seeking to ‘persuade the Biden administration’ that the companies’ activities remained of ‘great importance’ to the national security of both countries. Israeli officials reportedly were willing to commit to much closer supervision of the licensing of spyware software in exchange for a reprieve of the two companies. Thus far, the entreaties of Israel’s diplomats have not led to any policy changes by the U.S. government.

2.7. Conclusions

Even though the proliferation of digital technologies has undoubtedly facilitated the exercise of human rights in many ways, the overview of the trends presented in this chapter shows that it has also significantly expanded states’ toolkit for repression and social control. These technologies are actively deployed and shaped by many repressive regimes to their own strategic advantage. While China emerges as undisputed leader in this respect, harnessing sophisticated technologies to undermine human rights has occurred in all parts of the world. This includes both authoritarian and non-authoritarian regimes with advanced technological capacities, as well as less technologically developed states for which opportunities to import ‘off-the-shelf’ solutions from abroad have become increasingly available.

The spread of targeted surveillance technology, frequently used by repressive governments to track political opponents or monitor regime critics, continues to rise. NSO Group’s Pegasus software, linked to over 1,000 targets in over 50 countries, is emblematic of the breadth of the problem. But Pegasus is hardly the only commercial spyware vendor relied upon by governments. A range of commercial firms based in both democracies and authoritarian states—such as Cytrox, Cyberbit, Black Cube, Cellebrite, and RCS Labs—provide invasive tools to security services, intelligence agencies, and police departments, in pursuit of repressive objectives. As the global inventory of commercial spyware indicates, the number of countries procuring intrusive software has risen significantly, from 64 countries documented in the December 2020 version of the dataset to X countries today. This raises troubling questions about why efforts to stem the use of spyware continue to flounder. The answer is complicated, but geopolitical considerations, lucrative export markets, low political will among licensing countries, and regulatory loopholes have all contributed to allowing the commercial spyware market to sustain and thrive.

205 Haaretz (2018), Revealed: Israel’s Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays
206 Rest of World (2021), Inside Israel’s lucrative — and secretive — cybersurveillance industry
207 The New York Times (2021), Despite Abuses of NSO Spyware, Israel Will Lobby U.S. to Defend It
208 The New York Times (2021), Despite Abuses of NSO Spyware, Israel Will Lobby U.S. to Defend It
209 Even though this chapter and the whole study focus on threats posed by digital technologies to human rights, some advantageous uses of those technologies have been also flagged (such as encryption tools enhancing privacy and security online or communication technologies facilitating documenting and informing about human rights violations).
Another global trend emerging in recent years has been the expansion of sophisticated and ubiquitous data collection, especially a rise of biometric surveillance coupled with algorithmic decision-making (and concomitant challenges posed by algorithmic systems, such as the amplification of existing biases and a lack of transparency in ‘black box’ machine learning systems). Such mass-scale data collection, conducted in online and increasingly also offline spaces and used for monitoring, assessing, predicting and influencing people’s behaviour, has enabled a new mode of governance premised on profiling, sorting, and categorising populations. Besides this, more targeted tools for repression and social control are still widely used, including both technological, legal and extra-legal measures, a progressive share of which are ‘next generation toolkit’ tactics, which encompass practices that are more difficult to detect and hold people accountable for (compared to more ‘traditional’, blunt-force tactics). These tools and methods are increasingly being ‘exported’ beyond national borders in various ways, often by states, expanding their ‘cyber sovereignty’. This can be observed as another trend that facilitates further restrictions on the free flow of information online, which has become particularly detrimental in the context of the COVID-19 pandemic.

Notwithstanding the omnipresent character of widespread surveillance systems, which affect whole populations on a constant basis, the risk of use of new technologies for repression or control increases, in particular, in times of political tension, protests, demonstrations, armed conflicts and elections. Among the groups most often targeted are human rights defenders and other civil society activists, independent journalists, political opposition, and racial, ethnic and sexual minorities (including women, who are disproportionally affected and face specific types of cyber harassment). In 2020, this list could be expanded to also include healthcare workers who have been whistleblowing about the pandemic. However, when it comes to the proliferation of new technologies, such as digital identity systems, and the emergence of so-called ‘digital welfare state’, those that are increasingly the most threatened by the abuse of these tools include the poorest, migrants, and other most disadvantaged groups in society.

While the human rights situation in the context of new technologies has been gradually deteriorating over the past two decades, this process has been accelerated by the COVID-19 crisis. Surveillance-led responses to the pandemic have certainly brought the control powers of many states to a new level. They are, however, nothing but an extension of wider mega-trends that have emerged in recent years. These include, first of all, exploiting the state of emergency to justify an increase in long-term restrictions on fundamental rights. Just as in the case of many counter-terrorism measures adopted after the 9/11 attacks, there is fear that new surveillance regimes, introduced in response to the current health crisis, will eventually outlast the pandemic, and, after repurposing, become permanent solutions. Secondly, there is a risk of ‘technological solutionism’, wherein technology is seen as the only viable option to resolve any social issue, often without appropriate fit-for-purpose and proportionality assessments. Finally, ‘surveillance capitalism’ facilitates invasive harvesting and exploitation of personal data for profit by private actors, while also allowing state authorities access to these resources. In this context, it is symptomatic that ‘responses to COVID-19 have been largely based on the extraction of personal data stemming from public-private partnerships’. This illustrates another phenomenon of the digital era – an essential role of the private sector, which has been highlighted several times.

---


throughout this chapter. This includes companies developing and selling surveillance technologies and, in particular, a handful of big tech companies providing globally operating online platforms\(^{213}\). These companies exercise concentrated power over billions of people’s online expression, access to information and personal data, thanks to which, in many instances, they have become the gatekeepers of fundamental rights in the digital realm.

\(^{213}\) Among digital platforms, seven ‘super platforms’ – Microsoft, Apple, Amazon, Google, Facebook, Tencent and Alibaba – account for two thirds of the total market value of the world’s 70 largest platforms. See box above.
3. OVERVIEW OF THE INTERNATIONAL HUMAN RIGHTS FRAMEWORK

3.1. Introduction

This chapter presents an overview of recent developments in the human rights legal framework responding to current trends in the use of new technologies for repression and social control. It will highlight a selection of the most important international laws, standards, and other initiatives developed by intergovernmental bodies, both at the international and regional levels, such as the United Nations (UN), Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), the Organization of American States (OSCE), and the African Union (AU). It will assess the status of norm development in this area and will identify key gaps that should be confronted by human rights institutions in their future activities.

Legal instruments will be analysed in four categories pertaining to:

1) AI and algorithmic decision-making systems
2) modern surveillance
3) disruptions to free flow of information on the internet,
4) human rights responsibilities of private actors.

It has been widely recognised that human rights apply to the internet and other digital technologies. In 2012, the UN Human Rights Council adopted a ‘Resolution on the promotion, protection and enjoyment of human rights on the Internet’, for example, affirming that ‘the same rights that people have offline must also be protected online; in particular, freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice’. The main general international human rights instruments, therefore, including binding treaties such as the International Covenant on Civil and Political Rights (ICCPR) or the European Convention of Human Rights (ECHR) (see Box 6), while not specific to new and emerging technologies, in principle may be invoked to address the current human rights challenges posed by these technologies. This also applies to the key instruments protecting social, economic, and cultural rights (see Box 6) which, as already flagged in the previous chapter, are increasingly relevant in this context. It thus follows that design, development and deployment of any digital technologies are subject to the international human rights law three-part test, which requires that any measures restricting those rights must meet criterion of legality, pursue a legitimate aim, as well as be necessary and proportionate to achieve this aim. This means, in particular, that the use of digital technologies interfering with human rights must be always the exception, rather than the rule, must be provided in law, applied only in specific circumstances, and involve the least restrictive means possible.

At the same time, due to generic nature of the human rights treaties, in order to sufficiently meet emerging challenges pertaining to the use of new technologies and ensure their adherence to human

---

214 As also indicated in the Note on methodology, the analysis will be focused mainly on instruments adopted in the course of last 5 years.

215 UN Human Rights Council, Resolution on ‘the promotion, protection and enjoyment of human rights on the Internet’, A/HRC/20/L.13, 2012. The resolution started a series of subsequent resolutions with the same title adopted over the previous decade which have been progressing and consolidating its standards. There have been four resolutions adopted to date, the most recent one in 2018.

216 See for example Articles 8-11 of the ECHR.
rights standards, there is a need for more detailed guidelines. These guidelines can often be found in the 'soft law' instruments developed within different human rights institutions. Even though they do not have a binding force, they play an important role in interpreting and applying international norms, and may induce compliance with them by state and non-state actors. Moreover they have the potential to respond to the most actual problems, which – given the very dynamic nature of the field in question – is a significant asset of these documents. In light of a limited number of binding instruments specifically addressing repression and social control facilitated by the use of new and emerging technologies, the following chapter will thus focus to a great extent on the analysis of available soft law instruments. The analysis of this legal framework will be complemented by highlighting selected standards provided recently in the jurisprudence of the international courts.

Box 7: Main human rights international treaties and rights most affected by the use of digital technologies for repression and social control

<table>
<thead>
<tr>
<th>United Nations:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>International Covenant on Civil and Political Rights (‘ICCPR’)</strong>[^117]</td>
</tr>
<tr>
<td>Article 2 (3) – right to an effective remedy</td>
</tr>
<tr>
<td>Article 8 – right to work</td>
</tr>
<tr>
<td>Article 14 – right to a fair trial</td>
</tr>
<tr>
<td>Article 17 – right to privacy</td>
</tr>
<tr>
<td>Article 19 – freedom of expression</td>
</tr>
<tr>
<td>Article 21 – freedom of assembly</td>
</tr>
<tr>
<td>Article 22 – freedom of association</td>
</tr>
<tr>
<td>Article 25 – right to public participation</td>
</tr>
<tr>
<td>Article 26 – non-discrimination</td>
</tr>
<tr>
<td>• <strong>International Covenant on Economic Social and Cultural Rights (‘ICESCR’)</strong>[^118]</td>
</tr>
<tr>
<td>Article 2 (2) – non-discrimination</td>
</tr>
<tr>
<td>Article 6 – right to work</td>
</tr>
<tr>
<td>Article 9 – right to social security</td>
</tr>
<tr>
<td>Article 12 – right to the highest attainable standard of health</td>
</tr>
<tr>
<td>Article 13 – right to education</td>
</tr>
<tr>
<td>Article 15 (1) (b) – right of everyone to enjoy the benefits of scientific progress and its applications</td>
</tr>
</tbody>
</table>

| Council of Europe:                                                          |

[^117]: UN, 'Chart of signatures and ratifications of the International Covenant on Civil and Political Rights (‘ICCPR’).
[^118]: UN, 'Chart of signatures and ratifications of the International of the Covenant on Economic Social and Cultural Rights (‘ICESCR’).
Pegasus and the EU’s external relations

- **European Convention of Human Rights (ECHR)**
  - Article 5 – right to liberty and security
  - Article 6 – right to a fair trial
  - Article 8 – right to respect for private and family life
  - Article 10 – freedom of expression
  - Article 11 – freedom of assembly and association
  - Article 13 – right to an effective remedy
  - Article 14 – non-discrimination

- **European Social Charter (‘ESC’)**
  - Article 1 – right to work
  - Article 5 – right to organise
  - Article 11 – right to protection of health
  - Article 12 – right to social security
  - Article 14 – right to benefit from social welfare services
  - Article 19 – right of migrant workers and their families to protection and assistance
  - Article 20, Article E – non-discrimination

**Organisation of American States:**

- **American Convention on Human Rights (‘ACHR’)**
  - Article 8 – right to a fair trial
  - Article 11 – right to privacy
  - Article 13 – freedom of thought and expression
  - Article 14 – right of reply
  - Article 15 – right of assembly
  - Article 16 – freedom of association
  - Article 23 – right to participate in government
  - Article 24 – right to equal protection
  - Article 25 – right to judicial protection


---

219 Council of Europe, 'Chart of signatures and ratifications of the European Convention of Human Rights (‘ECHR’).

220 Council of Europe, 'Chart of signatures and ratifications of the European Social Charter (‘ESC’).

221 Organisation of American States, 'Chart of signatures and ratifications of the American Convention on Human Rights (‘ACHR’).

Article 3 – non-discrimination
Article 6 – right to work
Article 8 – trade union rights
Article 9 – right to social security
Article 10 – right to health
Article 13 – right to education
Article 14 – right to the benefits of culture

**African Union:**

- **African Charter on Human and Peoples’ Rights (‘ACHPR’)**

  Article 2 – right to freedom from discrimination
  Article 7 – right to fair trial
  Article 9 – right to receive information and free expression
  Article 10 – right to freedom of association
  Article 11 – right to freedom of assembly
  Article 13 – right to participate in government
  Article 15 – right to work
  Article 16 – right to health
  Article 17 – right to education
  Article 18 – protection of the family and vulnerable groups
  Article 19 – right of all peoples to equality and rights
  Article 20 – right to self-determination

### 3.2. AI and algorithmic decision-making systems

The development of AI has rapidly expanded over the last two decades. Alongside the increasingly sophisticated use of this technology, including as a tool enabling repressions and social control, setting appropriate standards for it has made it to the top of the agendas of several human rights organisations in recent years. The most comprehensive work has been done within the UN and CoE, while other regional organisations, such as the OSCE, have focused on more specific AI applications.

On the international level, a response to the growing prevalence of AI has been an essential element of the UN Secretary General’s efforts to strengthen international cooperation in the field of digital technologies. In 2018, the Secretary General released a strategy in which it seeks to align the use of AI with international human rights law in order to define how the UN system will support the use of this technology ‘to accelerate achievement of the 2030 Sustainable Development Agenda’. Additionally, the Secretary General has established the High-level Panel on Digital Cooperation (HLPDC). The aim of the HLPDC is to strengthen international and multi-stakeholder cooperation to

---

223 African Union, ‘Chart of signatures and ratifications of the African Charter on Human and Peoples’ Rights (‘ACHPR’).’
224 UN Secretary General, ‘Strategy on new technologies’, 2018.
contribute to the public debate on how to ‘optimise the use of digital technologies and mitigate the risks’\textsuperscript{225}. Based on the HLPDC 2019 landmark report\textsuperscript{226}, the Secretary General launched the ‘Roadmap for Digital Cooperation’\textsuperscript{227}. The Roadmap contains recommendations for concrete actions by diverse stakeholders in eight key areas, including ‘supporting global cooperation on artificial intelligence that is trustworthy, human-rights based, safe and sustainable, and promotes peace’. The Roadmap specifically provides potential mechanisms for cooperation, including the establishment of an advisory body on global artificial intelligence, as well as the appointment of a new ‘Tech Envoy’ in 2021.

At the same time, challenges related to the impact of AI technology have been increasingly addressed by UN human rights mechanisms, such as the Human Rights Council, General Assembly, and Special Rapporteurs, calling both States and business enterprises to ensure the protection of human rights when designing, developing, deploying and evaluating these systems. One of the prominent examples is the 2017 Human Rights Council resolution\textsuperscript{228}, which explicitly recognises the impact of profiling (which may involve the use of AI methods) to derive, infer or predict information about individuals for the purpose of evaluating some aspects about them. The Council also noted that ‘individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights’. Another very recent example is the 2020 General Assembly Resolution on ‘the right to privacy in a digital age’\textsuperscript{229}. Among its key aspects, it expresses concern with respect to the increase in the development of biometric data-driven AI systems, including the rise of biometric identity programmes and scoring systems across the world. Furthermore, in July 2019, pursuant to the adoption of the Human Rights Council’s resolution ‘New and emerging digital technologies and human rights’\textsuperscript{230}, the Council’s Advisory Committee was tasked with preparing a report to address the impact, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights, to be presented at the Council’s 47th session in June 2021\textsuperscript{231}. The aim of the study is also to map the progress made by the UN community in this area, as well the gaps in the current framework, with the prospect of further shaping the Council’s digital agenda with respect to current (and future) AI-powered and data-driven technologies.

More specific issues pertaining to the use of AI and algorithmic systems have been addressed by several UN Special Rapporteurs. These reports often contain in-depth analysis of the most current challenges in this area, as well as suggestions for new lines of interpretation and possible amendments to the human rights regime. They also explain how AI technology may affect a broad spectrum of human rights. The most comprehensive example is a report\textsuperscript{232} by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, examining the impact of AI on freedom of opinion, privacy, and non-discrimination. The report also proposes a human rights framework for the design and use of AI technologies by states and private actors. In particular, it urges for more transparency in the decision-making processes using algorithms and ensuring accountability.

\textsuperscript{225} UN, ‘Secretary-General’s High-level Panel on Digital Cooperation’, 2020.
\textsuperscript{227} UN Secretary General, ‘Roadmap for Digital Cooperation’, 2020.
\textsuperscript{229} UN General Assembly, ‘Resolution A/RES/75/176’, 2020.
\textsuperscript{231} UN Human Rights Council, ‘New and emerging digital technologies and human rights’.
\textsuperscript{232} UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ‘Report no. A/73/348’, 2018.
mechanisms that would allow the challenge of such decisions in effective ways. Another example is a report published by the Special Rapporteur on contemporary forms of racism, racial discrimination, and xenophobia. The report stresses that emerging digital technologies, driven by big data and AI, can reinforce and exacerbate existing inequalities, including those rooted in race, ethnicity, and national origin, in all areas of life, from education and employment, to healthcare and criminal justice. The report also corrects the misconception that these technologies are neutral and objective, by underlining that they are vulnerable for reproducing, whether intentionally or inadvertently, the discriminatory patterns of those developing, implementing, or using them. Last but not least, an important development responding to one of the most current challenges in the area of AI-powered biometric data collection systems is the report by the Special Rapporteur on human rights and extreme poverty. The Rapporteur addresses the emergence of digital identification systems – a problem that, so far, has been only briefly tackled in the human rights legal framework. It describes the negative impact of those systems on privacy, non-discrimination, as well as several social and economic rights, warning against a grave risk of ‘stumbling zombie-like into a digital welfare dystopia’. A noteworthy conclusion drawn from all the three reports is that ‘ethical approaches’, which often govern the development and application of emerging digital technologies, ‘must be pursued in line with international human rights law, and States must ensure that they do not function as a substitute for the development and enforcement of existing legally binding [human rights] obligations’.

In order to facilitate navigation though the key UN texts responding to challenges posed by new technologies, the UN has recently launched an online repository, the ‘United Nations Hub for Human Rights and Digital Technology’, gathering relevant standards, analysis, and recommendations emerging from its human rights mechanisms.

Among regional human rights organisations, as already flagged, CoE has taken the most advanced approach in the field of AI and algorithmic systems. In addition to its main human rights instruments, such as the ECtHR and ESC, the organisation has developed two other binding conventions, which are particularly important in the context of the use of AI. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (‘Convention 108’) was recently modernised by an amending protocol in 2018 (‘Convention 108’). The Convention ‘sets standards on the rights to privacy and data protection of individuals, regardless of technological evolutions’. It is also the first and, to date, the only international legally binding instrument dealing with data protection. The amending protocol added a number of new principles to address challenges posed by the processing of personal data through technological development, the increasing flow of personal data, and the globalisation of processing operations. They include principles of transparency, proportionality, accountability, impact assessment, and respect for privacy by design. It also added new data subjects’ rights, such as the right not to be subject to a decision significantly affecting a person based solely on an automated processing of their data, and the right to obtain knowledge of the reasoning underlying

---

233 UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, op. cit.
234 UN Special Rapporteur on extreme poverty and human rights, op. cit.
235 UN Special Rapporteur on extreme poverty and human rights, op. cit., par. 72.
236 UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, op. cit.
239 Council of Europe, Chart of signatures and ratifications of the Convention 108+.
240 Council of Europe European Committee on Crime Problems (CPDC), Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law, 2020.
such data processing where the results of this processing are applied. These new rights and principles are of particular importance in relation to the profiling of individuals and automated decision-making.

The process of modernisation for ‘Convention 108’ was carried out in parallel with other reforms to international data protection instruments, and alongside the reform of EU data protection rules, with the aim of ensuring consistency between both legal frameworks. As a result, Convention 108+ is mostly aligned with the EU General Data Protection Regulation provisions. Given that the Convention has been ratified by all CoE members and that is open for accession by states that are non-Contracting Parties of the CoE\(^{241}\), as well as by international organisations, it has the potential to set global standards and serve as a vehicle for promoting a data protection approach consistent with the EU legal framework at global level\(^{242}\). The text of the Convention has been complemented by several guidelines developed by the Consultative Committee (‘T-PD’) established by the same treaty, which specify the application of its provisions to concrete situations, including in the context of AI and data protection\(^{243}\), and big data\(^{244}\).

The CoE’s second binding international instrument particularly relevant for this study is the Convention on Cybercrime\(^{245}\) (‘Budapest Convention’). The Convention is important for criminalising offences against and by means of computers, for procedural powers to investigate cybercrime and secure electronic evidence, as well as for effective international co-operation in this area. It serves as a guideline for any country developing comprehensive national legislation against cybercrime. At the same time, the Convention is fully applicable to acts carried out or facilitated by AI systems, such as DDoS attacks or identity theft. The Budapest Convention is supplemented by a Protocol on xenophobia and racism committed through computer systems, while a new Protocol to the Budapest Convention on enhanced co-operation on cybercrime and electronic evidence is being prepared and may become available in 2021.

Furthermore, there has been a growing body of non-binding instruments developed by CoE institutions, which specifically tackle different applications of AI and their human rights impact. The most prominent examples are two recent documents adopted by the Committee of Ministers: the Recommendation on the human rights impacts of algorithmic systems\(^{246}\) and the Declaration on the manipulative capabilities of algorithmic processes\(^{247}\). Moreover, a set of recommendations for national authorities concerning the use of AI in 10 main areas of action was adopted by the CoE’s Commissioner for Human Rights\(^{248}\). Lastly, in 2017, the Parliamentary Assembly (PACE) adopted a recommendation...

---

\(^{241}\) To date, eight non-CoE countries are parties to the Convention: Argentina, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay. To date the 2018 amending protocol modernising the Convention has been ratified by Mauritius.

\(^{242}\) Interview with Patrick Penninckx, Head of the Information Society Department of the Council of Europe, 08 January 2021.


\(^{244}\) Council of Europe Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing (CoE T-PD), ‘Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data’, 2017.


\(^{247}\) Council of Europe Committee of Ministers, Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes, 2019.

\(^{248}\) Council of Europe Commissioner for Human Rights, ‘Unboxing artificial intelligence; 10 steps to protect human rights’, 2019. The areas of action include: human rights impact assessment; public consultations; human rights standards in the private sector; information and transparency; independent monitoring; non-discrimination and equality; data protection.
on ‘Technological convergence, artificial intelligence and human rights’ \(^{249}\), followed by 7 reports in 2020 focusing on different AI-related thematic areas. They include the need for democratic governance of AI; the role of AI in policing and criminal justice systems; discrimination caused by AI; threats to fundamental freedoms; medical, legal and ethical challenges in the field of health care; consequences on labour markets; and legal aspects of ‘autonomous vehicles’.

Besides that, the work of the CoE in the area of AI includes a number of research studies and reports developed by different CoE’s specialised committees and expert bodies. One such example is the European Ethical Charter for the use of artificial intelligence in judicial systems \(^{250}\), adopted by the European Commission for the Efficiency of Justice (CEPEJ). The Charter refers specifically to risks arising from AI-driven systems of anticipation of decisions, or risk-assessment systems in the judiciary, setting key principles for their use in this field. Other examples are the study on ‘discrimination, artificial intelligence and algorithmic decision making’ \(^{251}\) commissioned by the European Commission on Racism and Intolerance (ECRI) or the Background Paper on ‘AI and the media’ \(^{252}\).

It should be also emphasised that CoE’s existing AI-related legal framework is likely to expand in the foreseeable future. Apart from several regulatory measures that are currently being considered in areas such as AI and criminal law \(^{253}\) and AI-driven discrimination \(^{254}\), there are also ongoing efforts to develop a (potentially binding) legal instrument tailored to the specific challenges raised by AI systems and aimed at providing a comprehensive legal framework in this respect. This would challenge the current picture of a mostly fragmented existing legal framework composed of instruments focusing on particular aspects of different AI systems, and provide a more ‘holistic’ approach.

At the European level, the CoE’s developments in AI are complemented by the recent work of the OSCE Representative on Freedom of the Media. This work focuses on the challenges posed by advanced automated tools and machine-learning systems in content moderation and distribution online \(^{256}\). The goal of the Representative’s efforts is to ultimately develop policy recommendations on the most effective ways to safeguard freedom of expression and media freedom when using AI technologies within four main thematic areas of concern; security, hate speech, media pluralism, and surveillance.

**Box 8: International human rights mechanisms undermined**

It should be flagged that the role of certain international human rights mechanisms in confronting repressive regimes has been undermined, as some authoritarian states have been gaining more influence on their agendas. Russia and China, the world’s leaders in harnessing digital technologies for repression and social control, are currently both members of the UN Human Rights Council, but

---


251 Zuiderveen Borgesius, F., op. cit.


255 CoE established the Ad-hoc Committee on Artificial Intelligence (CAHAI), which was tasked to examine the feasibility of a legal framework for the development, design and application of AI. See, CoE CAHAI, op. cit. p. 85.

256 OSCE Representative on Freedom of the media, **Impact of Artificial Intelligence**.
are believed to have used this and other UN forums as a ‘means of shielding themselves from criticism, promoting their own illiberal projects’, and ‘reshaping international legal standards in ways that advance their interests’. Both states have pushed for the adoption of a new global binding treaty on cybercrime, for example. This eventually resulted in a Russian-led resolution passed by the UN General Assembly in late 2019 which is an initiative that raises serious human rights concerns and ‘advances Russia’s long-standing goal to replace the Council of Europe’s Budapest Convention’. The new treaty would likely lack the standards balancing the interests of law enforcement and respect for fundamental rights provided by the Budapest Convention, instead facilitating the repression and censoring of political dissent.

Other human rights organisations, such as the CoE, also face challenges in some of their member states that weaken the efficacy of their response to the trend of backsliding in human rights and democracy. The most prominent examples can be observed in Russia and Turkey; countries which refuse to uphold many of the organisations’ legal standards and are among the leaders in failing to effectively implement the ECtHR’s judgments, instead taking measures to undermine the Court’s supremacy.

3.3. Surveillance in a digital age

The ‘Snowden revelations’ in 2013 have increased concerns about the negative impact of the interception of digital communications on human rights, and triggered numerous responses from different human rights institutions. In particular, surveillance has been a focus of several UN initiatives. A significant part of those responses has been built around the question of adapting the right to privacy to the challenges posed by new technologies. However, threats to freedom of expression, freedom of peaceful assembly, the right to non-discrimination and the right to effective remedy have been also addressed in this context.

At the UN level, the ‘Snowden revelations’ have triggered the emergence of ‘the right to privacy in the digital age’ discourse, which has led to numerous resolutions from the General Assembly and Human Rights Council. These documents reaffirm that human rights standards should apply to the interception of communications and collection of personal data, including certain types of metadata. It was concluded that aggregated metadata ‘can reveal personal information that can be no less

258 UN General Assembly (2019), 'Countering the use of information and communications technologies for criminal purposes', Resolution A/RES/74/247
sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity. This discourse also resulted in the establishment of a dedicated UN special procedures mandate on the right to privacy, which closed a significant gap in the institutional human rights protection framework. In their first report, the Special Rapporteur on the right to privacy outlined the main priorities issues pertaining to digital surveillance, as well as the role and responsibilities of companies to protect personal data. Governmental surveillance, and in particular developing oversight mechanism of these activities, has remained an important focus of his subsequent reports. The resolutions on the right to privacy in a digital age and the work of the Special Rapporteur have since been complemented by a number of thematic reports from the other UN Rapporteurs and the High Commissioner for Human Rights. In all those documents, UN institutions elaborated principles to ensure that mass surveillance is conducted consistently with international standards, including standards of legality, necessity and proportionality, as well as robust procedural safeguards, such as independent oversight and the right to an effective remedy. These developments have been complemented by similar standards established at the regional level, in particular within CoE institutions (with a particularly significant role of the European Court of Human Rights – ECHR), the Inter-American Commission on Human Rights, and the African Commission on Human and Peoples' Rights.

More recently, the international human rights legal framework has responded to more targeted and offensive forms of surveillance, such as government hacking, both in national and extraterritorial contexts. At the same time, different institutions have promoted confidentiality, encryption, and anonymity as fundamental mechanisms to ensure human rights in the digital era. This approach

---

265 UN General Assembly, 'The Right to Privacy in the Digital Age', Resolution 28/16, A/HRC/RES/28/16, 2015. The Special Rapporteur is an independent expert appointed by the Council to examine and report back on a country situation or a specific human rights theme. The Special Rapporteur is mandated to report on alleged violations of the right to privacy, including in connection with the challenges arising from new technologies.
272 ECHR, 'Fact sheet on mass surveillance case law', 2020.
274 UN High Commissioner for Human Rights, op. cit. 1028; UN General Assembly Resolution, A/RES/73/179, op. cit., 2018.
was confirmed by the ECtHR in one of its recent judgements. Access to encryption and anonymity tools has been considered particularly vital for the work of journalists, human right defenders, civil society, journalists, whistle-blowers, and political dissidents facing persecution and harassment.

Furthermore, the role of the private sector in the context of state surveillance has been increasingly addressed. Initially, the human rights standards in this respect focused on situations in which private companies faced pressure from public actors. These included instances of States demanding excessive access to the massive amounts of information collected and stored by telecommunications and internet service providers, compelling private entities to assist in hacking operations, or calling for mandated back doors in encrypted communications. More recent work addresses a growing industry of private surveillance tools (in particular, spyware hacking tools and facial recognition technology). Many institutions have called on both state and non-state actors to refrain from providing surveillance equipment to foreign governments with a record of serious human rights violations, in the absence of legal safeguards or oversight mechanisms put in place. The most comprehensive proposal for a legal and policy framework was provided by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, who called for an immediate moratorium on the global sale and transfer of surveillance technology until rigorous human rights safeguards are implemented.

While excessive surveillance of digital communications remains a valid challenge, the most recent trends in developing a legal framework respond to the use of emerging surveillance technologies that involve processing of biometric data. This phenomenon has already been noted by several human rights institutions and is likely to receive more attention in the future. A signpost for further developments in this area may be the recent standards regarding the use of facial recognition. In 2020, the UN Human Rights Council adopted a resolution specifically condemning the use facial recognition technology, alongside other digital tracking tools, in the context of the right to peaceful protests. The Council noted that these technologies create a chilling effect on the exercise of the right to protest by enhancing governments’ abilities to identify, monitor, harass, intimidate, and prosecute protesters. The Council, therefore, explicitly called on states to refrain from using facial recognition technology to arbitrarily observe individuals involved in peaceful protests. At the same time, unfortunately, it has not addressed the role of private sector actors, such as social media companies, in advancing respect for the right to peaceful assembly, even though they currently provide key tools for organising and covering demonstrations. Similar concerns regarding the use of facial recognition were expressed by

---

276 ECtHR, Engels v. Russia, 61919/16, 23 June 2020. The case concerned the blocking of access to the applicant’s website hosting information about filter-bypassing and anonymity-enhancing tools on the internet, such as VPN or the Tor browser, deemed dangerous by Russian authorities. In its judgements the ECtHR recognized the content-neutral nature of those technologies and rejected the argument that such technologies are solely used for extremist purposes, highlighting they may also serve legitimate purposes. It found therefore violation of, inter alia, Applicant’s freedom of expression.


280 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, op. cit., 2019.

281 Such as UN General Assembly, A/RES/77/179, op. cit., 2018; UN High Commissioner for Human Rights, op. cit., 2018.

the UN High Commissioner for Human Rights\textsuperscript{283} and the U.N. Human Rights Committee in the newly-adopted General Comment No. 37 on the right to peaceful assembly\textsuperscript{284}. At the same time, facial recognition has been addressed in other law enforcement contexts. It is significantly covered in a report published in November 2020 by the Committee on the Elimination of Racial Discrimination recommending steps to prevent and combat racial profiling by law enforcement officials, for example\textsuperscript{285}.

Furthermore, as already flagged in the previous chapter, several human rights institutions acknowledged the negative impact of the COVID-19 pandemic on the right to privacy and data protection. Some of the UN Special Rapporteurs explicitly noted in this context that ‘the virus is not just the cause of illness and death, it is also a pathogen of repression’\textsuperscript{286}, and that ‘we could have a parallel epidemic of authoritarian and repressive measures’\textsuperscript{287}. The current crisis has triggered unprecedented proliferation of human rights standards in the area of health-related surveillance systems. Several human rights institutions, both at the universal\textsuperscript{288} and European\textsuperscript{289} levels, adopted documents concerning the processing of health-related data for the purposes of combating the pandemic, addressing, among other things, the emergence of contact tracing apps. These documents point out the sensitive character of the processed data, and set minimal guarantees safeguarding rights to privacy and to protection of personal data that states should meet when deploying health surveillance mechanisms. They also emphasise that the emergency measures adopted in response the pandemic should not turn into standard practice. At the same time, the pandemic has increased the relevancy of pre-existing (but fairly recent) international standards and recommendations concerning the processing of health-related data. These include, for example, the CoE’s Committee of Ministers

\textsuperscript{283} These conditions include effective, independent oversight of its use; strict privacy and data protection laws; and full transparency about the use of image recordings and facial recognition technology in the context of assemblies.

\textsuperscript{284} UN Human Rights Committee, ‘General comment no. 37 on the right of peaceful assembly (article 21)’, 2020. Given that General Comments are important interpretive documents related to the human rights covered by the ICCPR, the new document has a significant potential to influence practical application of Article 21 by UN bodies. In particular, the Human Rights Committee often relies on General Comments in the course of monitoring implementation of the ICCPR by its State Parties, including examination of periodic reports by governments.


\textsuperscript{286} UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ‘Disease pandemics and the freedom of opinion and expression’, Report no. A/HRC/44/49, 2020.

\textsuperscript{287} S. Gebrekidan, ‘For autocrats and others, coronavirus is a chance to grab even more power’, New York Times, 30 March 2020.


\textsuperscript{289} While responding to other pandemic-related threats, the other regional human rights legal framework have not addressed this particular issue. At the European level, the relevant standards have been develop by mainly by the Council of Europe, including: (1) two Joint Statements ‘on the right to data protection in the context of the COVID-19 pandemic’ and on ‘digital contact tracing’ by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe; (2) CoE Secretary General, ‘Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis: A toolkit for member states available in different languages’, 2020; (3) CoE, ‘Digital solutions to fight COVID-19’, 2020, report analysing the impact on the rights to privacy and data protection of the measures taken to prevent the spread of the COVID-19 pandemic in the 55 African, Latin-American and European countries Parties to Convention 108.
3.4. Disruptions to free flow of information online

A growing body of findings and resolutions, both at the universal and regional levels, suggest that intentional disruptions to the internet violate international law. In 2015, in a joint declaration on freedom of expression and conflict situations, and UN and regional monitors of freedom of expression, declared that the ‘filtering of content on the Internet, using communications “kill switches” (shutting down entire parts of communications systems) are measures which can never be justified under human rights law’. At the UN level, the importance of access to online information has been confirmed in numerous documents. The landmark instrument specifically condemning internet shutdowns is the Human Rights Council Resolution from 2016. Since then, calls on states to refrain from imposing internet or telecommunications network disruptions have been repeated on several occasions. One of the most recent examples is the resolution of the Human Right Council, which expressed deep concern about the imposition of this measure as a means to undermine peaceful protests. The importance of the free flow of online information in the context of the right to peaceful assembly was also recently stressed by the ECHR.

Among other regional responses to internet shutdowns, given network disruptions have lately become more prevalent in Africa, it is particularly noteworthy to mention steps taken in this respect by the African Commission on Human and Peoples’ Rights. It specifically recognised that ‘universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression [and] access to information’ in a revised version of the Declaration of Principles of Freedom of Expression and Access to Information in Africa, which was adopted in 2019. Moreover, the African Special Rapporteur on Freedom of Expression and Access to Information expressed concern about the continuing trend of internet shutdowns in Africa, in particular in Chad, Sudan, the Democratic Republic of Congo, Gabon, and Zimbabwe. Furthermore, a landmark judgment was delivered by the Community Court of Justice of the Economic Community of West African States (ECOWAS), which held that the Togolese government violated the applicants’ right to freedom of expression by shutting down the internet during protests in September 2017. Still,

---

292 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/44/49, op. cit., 2020.
293 Available at: www.osce.org/fom/66176.
297 ECtHR, Kablis v. Russia, 59663/17, 30 April 2019. The ECtHR held the prohibiting the Applicant from holding a demonstration, and ordering the removal of his online posts about it, as well as entire social media account, violated his rights to freedom of expression and public assembly.
despite all these efforts, internet shutdowns remain on the agenda of human rights institutions as one of the key challenges for freedom of expression for the next decade\textsuperscript{301}.

Apart from internet shutdowns, other forms of disruption to the dissemination of online information have been condemned in international law, including imposing measures to unlawfully or arbitrarily block content or take down media websites (including via DDoS attacks)\textsuperscript{302}. A comprehensive set of standards concerning blocking access to websites was recently provided by the ECtHR in four cases against Russia\textsuperscript{303}. Moreover, human rights institutions developed recommendations preventing governments from putting undue pressure on internet intermediaries (including large online platforms) to remove content or enable excessive access of the authorities to user data. These recommendations include certain procedural guarantees safeguarding transparency, legality, necessity and proportionality of the governments' demands, including (in principle) an obligation to obtain an order from a judicial authority (or other independent authority whose decisions are subject to judicial review), as well as establishing a mechanism for an effective remedy\textsuperscript{304}. Both with respect to content restriction and disclosures of personal data, there should be a reporting obligation for states to publish comprehensive information on the number, nature, and legal basis of such orders. International standards also explicitly prohibit States to exert pressure on internet intermediaries through non-legal means. In addition, demands to access personal data stored by internet intermediaries should meet international data protection principles prescribed, for example, in Convention 108+, such as purpose limitation, data minimisation, storage timelimitations, data security, and data subjects’ right. States should ensure that the right to confidentiality of all private communications extends not only to the content of the communication, but also to metadata.

In 2020, several human rights institutions developed guidelines addressing specific threats to freedom of expression online posed by the COVID-19 pandemic, emphasising the need to protect access to accurate and reliable information in times of crisis. The most elaborate document is the report of the UN Special Rapporteur on freedom of expression, which focuses on 5 challenges during the pandemic:

1. access to information held by public authorities;
2. undisturbed access to the Internet;
3. protection and promotion of independent media;
4. the need to counteract public health disinformation;
5. the rise of public health surveillance\textsuperscript{305}.

In addition to freedom of expression risks, the Rapporteur also highlighted the negative impact of network disruptions imposed in the course of the pandemic on the right of everyone to enjoy the


\textsuperscript{302} For example, in its resolution 39/6, the UN Human Rights Council condemned these activities in the context of journalistic work.

\textsuperscript{303} ECtHR, OOO Flavus and Others v. Russia, 12468/15 and 2 others; Bulgakov v. Russia, 20159/15; Engels v. Russia, op. cit.; Vladimir Kharitonov v. Russia, 10795/14 (all judgments delivered on 23 June 2020).


\textsuperscript{305} UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2020), ‘Report: Disease pandemics and the freedom of opinion and expression’, A/HRC/44/49.
benefits of scientific progress, protected under article 15 (1) (b) of the CESCR. The importance of access to the Internet during the crisis in the context of economic, social and cultural rights has also been emphasised in the resolution of the Inter-American Commission on Human Rights and in the joint statement with IACHR Special Rapporteur for Freedom of Expression. At the same time, freedom of expression monitors from the UN, OSCE and OAS addressed the problem of punitive actions against journalists for pandemic-related speech, and stressed that press freedom must not be undermined by measures to counter disinformation about COVID-19. In particular, penalisation of disinformation should not be accepted as a proportionate measure, failing to achieve its goal of tamping down information while instead deterring individuals from sharing what could be valuable information.

At the same time, freedom of expression monitors from the UN, OSCE and OAS addressed the problem of punitive actions against journalists for pandemic-related speech, and stressed that press freedom must not be undermined by measures to counter disinformation about COVID-19. In particular, penalisation of disinformation should not be accepted as a proportionate measure, failing to achieve its goal of tamping down information while instead deterring individuals from sharing what could be valuable information.

Similar concerns have been expressed in this respect by the CoE’s Commissioner for Human Rights.

Additionally, one of the main threats to online free expression recognised by human rights institutions is different forms of cyberviolence, in particular state-sponsored harassment campaigns. Until recently, the work of international organisations in this area had focused on developing general standards on combating hate speech or increasing protection for the most vulnerable groups, such as journalists. In recent years, however, there has been an increasing number of international initiatives addressing discrimination and violence against women in the digital context. In 2017, the UN General Assembly unequivocally condemned all ‘specific attacks on women journalists in the exercise of their work, including sexual and gender-based discrimination and violence, intimidation and harassment, online and offline’. The problem was tackled more extensively in the 2018 resolution of the Human Rights Council, and in the report of the Special Rapporteur on violence against women, its causes, and consequences. Important work has been done in this area, not only in terms of setting policy guidelines, but also in advancing research about the problem by UNESCO and the OSCE.
Representative on Freedom of the Media 317 (in particular, with respect to online violence against female journalists). In addition, two binding instruments developed within the Council of Europe, namely the Budapest Convention and the Istanbul Convention 318, should be flagged as important developments in the context of countering gender-based cyberviolence, even though it has been pointed out that these instruments may not address the specificities of violence in cyberspace in a satisfactory manner 319. By the same token, the CoE’s Committee of Ministers Recommendation on preventing and combating sexism can be also relevant 320.

Last but not least, while governments across the world still increasingly resort to shutting down the internet, other network disruptions, or online harassment campaigns, recently many human rights institutions have been turning their attention to threats to free speech related to the activity of non-state actors, in particular large online platforms. In the joint declaration by freedom of expression monitors from the UN, OSCE, OAS and ACHPR, ‘a private control over online information flow’ is considered one of the main challenges to the freedom of expression for the upcoming decade 321. At the same time, online platforms are in a ‘unique position to prevent or mitigate risks that may be inflicted by users’ illegal activity’ 322. At the moment, the vast majority of international standards which aim to address this problem focus on content moderation 323. In particular, there are recommendations for States on how intermediaries’ liability regimes should be shaped at the national level. According to those standards, while in principle intermediaries should cooperate with states to effectively secure the restriction of illegal content, they should also benefit from limited liability regimes. States should refrain from imposing obligations to use general content monitoring to pro-actively identify illegal user-generated content in national laws 324. Moreover, there are recommendations regarding the need to adhere online platforms’ internal policies to international freedom of expression standards, and provide ‘due process’ safeguards for users, as well as independent, external oversight of the take down decisions, including those made on the basis of the companies’ own terms and conditions 325. There is also a growing body of recommendations concerning the use of automation in content moderation. These refer, in particular, to the need for increasing transparency of algorithms used for this purpose, and to possible limitations for their application due to the ‘deleterious impact’, which a sole reliance on these tools may have on human rights 326. Moreover, as already flagged in the section on AI, human rights institutions have been increasingly addressing the use of algorithms for broader content 327.

---


324 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, op. cit., 2018; COE Committee of Ministers (2018), op. cit., 2018.

325 Ibidem.

governance which enables companies to ‘curate search results and newsfeeds as well as advertising placement, organising what users see and when they see it’.

3.5. Human rights and private actors

A transformative feature of the digital communications environment which transpires not only from the previous section, but the entire study, is the impact of private companies on human rights in digital space. As already mentioned, this applies especially to internet intermediaries, including, in particular, large, dominant online platforms operating globally, such as social media or search platforms. Additionally, the international human rights legal framework puts a spotlight on the private surveillance tools industry. The role of both kinds of these non-state actors has been emphasised in most of the issue-specific instruments discussed earlier in this chapter (however, as highlighted above, some of these instruments still fail to appropriately address the significance of private sector).

Much of the literature on human rights considers that the framework applies primarily to state actions. The states’ duties extend beyond the obligation to respect, however, and also include ‘positive’ measures to protect the enjoyment of rights against threats emanating from private actors. In the context of AI, for example, this implies that ‘states can meet this obligation through legal measures to restrict or influence the development and implementation of AI applications, policies regarding the procurement of AI applications from private companies by public sector actors, self-and co-regulatory schemes or building of capacity in private sector companies to recognise human rights in their corporate endeavours’.

Similarly, with respect to the export of surveillance technologies by private actors, states should have export control regimes in place, which ‘assess the legal framework governing the use of this technology in the destination country, the human rights record of the proposed end user, and the safeguards and oversight procedures in place for the use of surveillance powers. Human rights guarantees need to be included in export licensing agreements’.

Even though international human rights law acknowledges that states are the prime duty bearers in the context of human rights obligations, many standards recognise that the private sector also bears a responsibility to respect human rights. The main global standard in this respect has been provided by the UN in the Guiding Principles on Business and Human Rights. The Guiding Principles offer a universal, non-binding vehicle for applying human rights standards to corporations. They build upon

327 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/73/348, 2018, Ibidem; see also: COE Committee of Ministers, Ibidem, 2018.


330 See e.g., article 2 (1) of the ICCPR and also ‘The Guiding Principles on Business and Human Rights’ (‘State duty to protect human rights’).


and help to operationalise the 2008 ‘Protect, Respect and Remedy’ Framework developed by the UN Special Representative on the issue of human rights and transnational corporations and other business enterprises, corresponding to three pillars for action (see Box 8).

Box 9: Three pillars of the of the ‘Protect, Respect and Remedy’ Framework

<table>
<thead>
<tr>
<th>I. Protect</th>
<th>focusing on states’ duty to protect against human rights abuses by third parties, including business, through appropriate policies and regulation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>II. Respect</td>
<td>focusing on corporate responsibility to respect human rights which means that companies must inter alia prevent and mitigate human rights harms, develop policies that promote human rights, carry out due diligence to assess human rights risks and address adverse impacts that occur.</td>
</tr>
<tr>
<td>III. Remedy</td>
<td>focusing on both State and business responsibility to provide victims with an access to effective remedy, both judicial and non-judicial.</td>
</tr>
</tbody>
</table>

The Guiding Principles apply to all kind of businesses, including online platforms and other tech companies. However, since they are not specific to the tech industry, companies may face practical problems with their effective application. In order to facilitate application of the principles to this particular sector, several human rights documents include guidelines on both substantive standards and processes for implementing them, for example in the algorithmic systems domain. In addition, there are other ongoing efforts within the UN, such as the ‘Business and Human Rights in Technology Project’ (‘B-Tech Project’) which applies the Guiding Principles to digital technologies. Another initiative is the ‘Accountability and Remedy Project’ launched in 2014 by the UN High Commissioner for Human Rights. It aims to deliver workable recommendations for more consistent implementation at the national level of the guiding principles in the area of access to remedy in relation to non-state actors, including, for example, with respect to abuses of the right to privacy in the digital space. To date, three phases of the project have been completed in which recommendations concerning establishing or improving three categories of grievance mechanisms referred to in the UN Guiding Principles were developed:

- judicial mechanisms;
- state-based non-judicial mechanisms;
- non-state based grievance mechanisms.

Following up on that work, the UN High Commissioner for Human Rights began work on a fourth phase in 2020 focusing on enhancing the accessibility, dissemination and implementation of the findings and recommendations made in the previous phases.

At the same time, there are ongoing efforts at the UN to complement the Guiding Principles on Business on Human Rights with an international legally binding treaty regulating corporate liability.

---

335 Information on the B-Tech Project is available here.
336 OHCHR Accountability and Remedy Project; the Project has received multiple mandates from the Human Rights Council (Resolutions 26/22, 32/10, 38/13 & 44/15).
337 The elaboration of the Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises was mandated in 2014 by Resolution 26/9 of the UN Human Rights Council. The Second Revised
Pegasus and the EU’s external relations

for human rights abuses. The currently negotiated ‘Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises’ addresses the need to increase the effectiveness of human rights protections in this area, which at the moment is undermined by its non-mandatory nature and lack of a central mechanism to ensure their implementation. The limited effectiveness of this framework can indeed be observed specifically in the technological domain. On the one hand, a growing number of companies are making formal commitments to human rights, including explicitly to upholding the standards established in the UN Guiding Principles. According to the Ranking Digital Rights Corporate Accountability Index 2020 (see Box 7) all the U.S.-based large online platforms (see Box 4 in Chapter 3) performed relatively well in 2020 when it came to declaring respect for human rights principles (while their Chinese counterparts, even though ranked much lower, also made some progress in this respect). On the other hand, however, most companies scored poorly on practical implementation of these commitments, including human rights due diligence, regular engagement with civil society, and offering effective remedy mechanisms for addressing human rights harms.

Box 10: Civil society and multistakeholder initiatives on business & human rights in a digital space

In addition to the above-mentioned standards, there are a range of civil society and multistakeholder initiatives that have developed recommendations that support operationalising the UN Guiding Principles for companies in the digital environment or monitoring their effective implementation. These include, for example:

- **Global Network Initiative** – A multistakeholder initiative dedicated to advancing human rights in the information and communications technology sector. It has developed a set of principles (‘GNI Principles’) and implementation guidelines to ‘guide responsible company, government, and civil society action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users’.

- **Toronto Declaration** – A set of standards protecting human rights in the age of artificial intelligence, focusing on protecting the rights to equality and non-discrimination in machine learning systems, developed by civil society organizations working on digital rights.

- **Santa Clara Principles** – A set of standards outlining minimum levels of transparency and accountability that online platforms should provide around their moderation of user-
generated content\textsuperscript{345}, drafted by a group of organizations, advocates, and academic experts who support the right to free expression online.

- **Ranking Digital Rights Corporate Accountability Index**\textsuperscript{346} – An index evaluating the world’s most powerful digital platforms and telecommunications companies on their disclosed policies and practices affecting users’ rights to freedom of expression and information and privacy.

### 3.6. Conclusions

The recent developments in the human rights framework described in this chapter are a sign of a growing awareness among the international community of how technologies affect societies and almost every part of our day-to-day lives. They also demonstrate an increasing caution and healthy scepticism towards application of new technologies, as it has been acknowledged that, alongside potential advantages, there may be unintended adverse consequences, or sometimes the potential to be used as deliberate tools of repression. The existing legal framework tackles many threats identified in Chapter 3, including practices described as part of a ‘next generation repression toolkit’. In particular, it responds to problems such as internet shutdowns and other network disruptions, mass and biometric surveillance, government hacking through spyware, export of surveillance tools, or cyber harassment. At the same time, there are fields that can be improved or should be further addressed. The main conclusions, built on the analysis of existing norms and interviews with different stakeholders\textsuperscript{347}, have been listed below with the aim of informing discussions on future development of human rights protection in the digital era.

Among the new and emerging technologies, which may be used for repression and social control, AI and algorithmic decision-making systems have dominated the most current agendas of human rights organisations. Building upon general principles on personal data protection, the right to privacy, freedom of expression or non-discrimination, there have already been several soft law instruments and other initiatives that aim to respond to the certain threats posed by those technologies. The existing instruments focus mainly on particular technological applications of AI technologies or their impact on selected rights. Still, there are gaps in the current level of protection. Most importantly, a comprehensive, international legal instrument, specifically tailored to challenges posed by AI, is lacking\textsuperscript{348}. At the same time, there are already advanced debates on how this gap could be filled. There seems to be a consensus that such an instrument should be technology neutral and reflect paradigm shifts in AI technologies. In particular, it should incorporate human rights safeguards into the entire life cycle of these technologies, including their design, deployment and implementation, as well as to the entire ‘datafication cycle’ (a process whereby data about individuals and things is collected, transmitted, and used to guide decision-making in the real world\textsuperscript{349}). There is also an urgent need to further address the causes and impact of unintended bias and discrimination resulting from certain algorithmic and automated decision-making based on AI\textsuperscript{350}. It is particularly important in contexts such


\textsuperscript{346} Ranking Digital Rights, op. cit.

\textsuperscript{347} See Section 2.2. ‘Note on the methodology’ and Annex 7.2.

\textsuperscript{348} Council of Europe Ad Hoc Committee on Artificial Intelligence (CoE CAHAI), op. cit., 2020.

\textsuperscript{349} Interview with representative of international institution, 14 January 2021, CoE CAHAI (2020), ibidem.

\textsuperscript{350} UN Secretary General, ‘Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights’, A/HRC/43/29, 2020.
as predictive policing in law enforcement, distribution of access to vital products and services or certain privileges, and content governance online\textsuperscript{351}.

It should also be noted that new technologies, in particular those driven by AI, challenge the traditional concept of groups particularly vulnerable to human rights violations, and (to some extent) the whole concept of a ‘victim’ and ‘harm’ under human rights framework. On the one hand, the analysis of trends in Chapter 2 has shown that ‘traditional’ groups such as racial, religious, or sexual minorities, political opposition, or civil society activists remain the primary targets. On the other hand, the rise of, for example, digital welfare systems, has exposed new, but also more ‘blurred’, groups that may be particularly affected, such as the poor and other disadvantaged categories. In addition, measures such as algorithmic surveillance affect large parts of populations, not whole societies, and thus the targets can no longer be specifically identified. Moreover, the individual harm is more difficult to grasp and often practically impossible to be documented or proved. The traditional notions of ‘victim’ status or ‘harm’ may therefore be insufficient to meet the current challenges posed by new technologies, and may require revisiting in order to offer effective human rights protection to individuals in a digital age\textsuperscript{352}.

At the same time, there has been an increasing recognition among human rights institutions that new and emerging technologies may impact a broad range of human rights. Such a ‘holistic’ approach, rather than focusing on the impact on particular rights, which were more prevalent in the past, should be kept and further expanded. It is difficult, for example, to comprehensively address the threats related to cyberviolence without considering at the same time human rights implications of automatisation of online content moderation. Similarly, one should not push for improving responses to cybercrime, including effective identification of perpetrators of online crimes, without due regard to the value of anonymity and encryption in certain contexts. All these issues, at least to some extent, have been addressed in the existing human rights framework, but often in a fragmented way, without taking into consideration interrelations between them\textsuperscript{353}. Moreover, while to date civil and political rights were under the spotlight of the human rights community, it has become clear that a number of social, economic and cultural rights are also severely affected. Technology-related violations of these rights have become particularly apparent alongside proliferation of digital identity systems and in the context of the COVID-19 pandemic. In light of these developments and in line with the ‘holistic’ approach, social, economic, and cultural rights should be given more prominence in future human rights organisations’ agendas on new technologies\textsuperscript{354}.

Government deployment of spyware surveillance and digital forensics technology poses unique challenges. In rare situations, based on principles of necessity, proportionality, legitimacy, and lawfulness, governments may be permitted to use these measures. However, because of the wide adverse impact of spyware hacking, experts caution that targeted surveillance should be limited to “the most exceptional circumstances, in strict adherence with the requirements of international law”\textsuperscript{355}.


\textsuperscript{352} E. Kosta, ‘Algorithmic state surveillance: Challenging the notion of agency in human rights’, Regulation & Governance, 7 July 2020.

\textsuperscript{353} An example may be the recent UN Human Rights Council Resolution on Freedom of opinion and expression, which fails to address the impact of surveillance technologies, which cause significant chilling effect on freedom of expression (A/HRC/44/12).


\textsuperscript{355} UN Secretary General A/HRC/43/29, 2020, op. cit.

UN General Assembly, “The right to privacy in the digital age”, A/HRC/51/17
complicating factor is that many of the jurisdictions documented to have used or to be using spyware lack essential legal safeguards and do not have “clear, precise, publicly available laws” to govern hacking operations. What is particularly problematic are the “necessity and proportionality” pillars used to determine lawful use of spyware. While it may be easier for governments to justify certain hacking operations under the legitimacy standard – for example, deployed for operations to counter terrorist threats or maintain public order – it is much harder for governments to argue that these operations are necessary for the well-being of a particular country, represent the least intrusive most effective option, and also are a proportional response to the threat at hand.

For countries that have basic legal frameworks in place related to spyware, their statutes frequently rely on “overly broad or outdated laws” enacted prior to the development of modern digital technologies. What this adds up to is a very narrow set of legal exceptions that severely limit the number of cases where a government would be justified in using intrusive software to carry out surveillance against certain individuals or entities. As OHCHR states in the 2022 right to privacy in the digital age report, spyware measures “should be a last resort,” used only after “all less intrusive measures” have been exhausted and then should be “strictly limited in scope and duration.” These measures should be additionally subject to vigorous oversight, prior judicial approval, and independent monitoring to ensure human rights compliance. Finally, it should be noted that while hacking by governments can be justified in exceptional circumstances, the use of malicious software by private individuals or businesses against other counterparts is never justified.

In 2020, several human rights institutions developed guidelines addressing human rights threats posed by the COVID-19 pandemic, including those specifically related to the use of new technologies. In particular, they address the rise of health-related surveillance tools, such as mobile phone apps developed to tackle the pandemic, and a number of freedom of expression risks. A concerning trend of governments using the pandemic as a pretext to expand general surveillance in order to increase repression and social control was also noted. Looking to the future, the important role of the human rights community is to further monitor the situation and, as more evidence is available, continue assessment of COVID-19-related surveillance’s impact on human rights. In particular, it is important to urge that any current measures justified by governments through the health emergency remain temporary, time-limited, and take the least intrusive approach. Based on lessons learned during the current crisis and keeping in mind that pandemics may become episodic features of contemporary life, human rights organisations should also work towards more sustainable and evidence-based guidelines on health-related emergency measures to prevent the future abuse of surveillance technologies. At the same time, it has to be acknowledged that COVID-19 pandemic is a point of no return. It has most likely already contributed to a wider normalisation of surveillance, and thus the human rights community will have to confront challenges arising from that fact.

It has been also widely recognised that an effective human rights response to the challenges posed by new technologies will not happen without the involvement of private companies. This applies, in particular, to large, dominant online platforms that, by exploiting huge volumes of user data for their business-driven purposes and exercising private control over the flow of online information, hold enormous power in the digital environment, posing systemic threats to a wide range of human rights. At the same time, the role of other corporations in facilitating human rights violations related to the use of new technologies, such as those producing and selling surveillance equipment, should not be

---

356 UN General Assembly, “The right to privacy in the digital age”, A/HRC/51/17
357 UN General Assembly, “The right to privacy in the digital age”, A/HRC/51/17
358 UN General Assembly, “The right to privacy in the digital age”, A/HRC/51/17
overlooked. It is therefore urgently required of the private sector in the technological domain to act responsibly in mitigating the risks that their activities may have on human rights. Currently, the main global standard for applying human rights responsibilities to corporations has been provided by the UN Guiding Principles on Business and Human Rights. However, the Guiding Principles do not sufficiently address the specificities of new business models that have arisen in the new technologies sector, which may impede their effective application in this area. It is therefore important to develop more practical guidance on the application of the Guiding Principles to digital technologies. Those developments should build on existing initiatives, such as the B-Tech Project or ‘ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights’ published by the European Commission. Additionally, improving mechanisms of cooperation and information-sharing between human rights community and technological companies could also facilitate better adherence of those actors to their human rights responsibilities. The non-binding character of this framework remains an impediment to fully effective protection against human rights abuses related to the activities of the private sector, which is why ongoing efforts to develop a mandatory international legal instrument (such as the UN Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises) should be supported.

Apart from enhanced cooperation with the corporate sector, it is also essential to include other actors, particularly from civil society and academia. First of all, with their field experience and expertise, these actors may inform international responses to the actual negative impacts of new technologies at the national level. Second, given the already existing initiatives, such as the Toronto Declaration or Santa Clara Principles, they may provide valuable input to the process of looking for solutions to the problems diagnosed in this section. Thirdly, this community also has a significant role in promoting international human rights standards in domestic policymaking.

Moreover, human rights should not give way to ethical frameworks in the field of new technologies. While ethical frameworks have been increasingly prevalent, in particular in the AI domain, and may assist with working through particular challenges regarding concrete applications of this technology, they do not provide tangible protection for individuals. Therefore, they should not be considered a substitute for a binding, actionable, and well-established human rights legal framework. Both public and private actors developing and implementing ethical codes on AI should ensure that they are grounded in human rights principles, in line with guidance that should be provided, in this respect, by the human rights community.

There are also other kinds of gaps that impede tackling the challenges posed by new technologies. Responding to complex human right issues created by these technologies requires adequate resources, including, in particular, human resources to close the ‘knowledge gap’ between legal/human rights and technology experts. Human rights bodies should therefore encourage more participation from diverse actors, including technology experts and representatives of the private sector who design and produce technologies. It is necessary to build new principles that can accommodate more varied and comprehensive perspectives. Additionally, as new technologies

359 Interview with representative of international institution, 14 January 2021.
363 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/73/348, op. cit., 2018.
364 Interview with representative of international institution, 14 January 2021.
continue to unfold; this goal will not be met without allocating appropriate funds to facilitate further research in this area.\textsuperscript{365} Last but not least, some respondents in our study have emphasised that the key limitation of the human rights legal framework is not the question of its content, but of its often-ineffective application at the national level, with limited avenues for remedies for harm caused by human right violations.\textsuperscript{366} More specifically, in the context of the dynamic expansion of technologies, it has been suggested to establish an emergency-response mechanism that would allow a more timely reaction of the international community to emerging digital threats.\textsuperscript{367} Finally, the increasing influence of non-democratic regimes on the agenda of human rights institutions and on the shape of international legal standards further undermines the role of this framework.

\textsuperscript{365} Interview with representative of international institution, 14 January 2021.

\textsuperscript{366} Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020; Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now, 6 January 2021; Diego Naranjo, Head of policy, European Digital Rights, 08 January 2021; Jonathan McCully, Legal Adviser, Digital Freedom Fund, 17 December 2020.

\textsuperscript{367} Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020.
4. **THE EU’S DEMOCRACY AND HUMAN RIGHTS TOOLBOX**

This chapter lays out the policy instruments the EU has at its disposal to support democracy and human rights across the world, paying particular attention to those parts of its toolbox related specifically to the effects of digital repression. The chapter describes how the EU has deployed the different parts of its policy toolbox in recent years. It concludes with an assessment of these policy approaches and relates them to the multiple digital trends summarised in the foregoing chapters. The chapter finds that the EU has moved up a gear in its efforts to tackle digital challenges, but that the worrying trends described in Chapter 3 require it to work even harder to improve its toolbox. While previous chapters highlight the spread of a multi-faceted set of digital problems, the EU’s external toolbox has improved mainly on select elements of this; in particular, it has focused on the use of digital technologies for repression against democracy and human rights actors within civil society, the export of security surveillance equipment, and the transnational use of digital tactics against the EU itself. The more subtle forms of social control, advanced AI techniques, or health-related controls described in Chapter 3 have so far proven less amenable to being incorporated fully into foreign policy instruments.

4.1. **General evolution of the EU toolbox**

4.1.1. **Evolution of the core toolbox**

The EU has been adding to and fine-tuning its array of human rights and democracy policy instruments for nearly three decades. The Union first began to develop funding instruments on these issues within its external aid in the early 1990s. From the mid-1990s, the EU insisted that all third-country partners sign a so-called ‘essential elements’ clause as part of formal contractual agreements with the Union, committing them to respect democratic norms and human rights standards. In the 1990s and early 2000s, the EU’s commitments intensified as democracy spread globally, and the Union offered assistance to the many governments that committed themselves to political reform. As this stage, the enlargement process in Central and Eastern Europe was perhaps the most significant policy tool for advancing democratic reforms and human rights protection, and it seemed for a while that this would also extend its leverage into the Western Balkans and Turkey.

In the last decade, EU policy commitments and instruments have continued to develop at a formal level, even as international trends began to look less favourable for democracy. Governments agreed a set of Council Conclusions in 2009, which reiterated the commitment to the promotion and protection of human rights\(^{368}\). EU development cooperation became more political in its stated aims, with the European Commission’s Agenda for Change placing support for democracy and human rights at the heart of development aid\(^{369}\). In 2012, the EU agreed a Strategic Framework and Action Plan on Human Rights and Democracy\(^{370}\), building on the joint Communication issued by the Commission the year before\(^{371}\). Democracy support was also formally built into an array of external policy frameworks.

---


such as the European Neighbourhood Policy\textsuperscript{372} and the EU Consensus on Development\textsuperscript{373}. From 2016, EU Delegations were obliged to report on Commission and Member State initiatives in support of democracy and human rights in their respective countries\textsuperscript{374}.

Although the 2016 Global Strategy centred mainly on security issues, it did formally confirm EU support for human rights and democratic norms around the world. EU foreign policy would aim to foster ‘resilient states’, based on a conviction that ‘a resilient society featuring democracy, trust in institutions, and sustainable development lies at the heart of a resilient state’\textsuperscript{375}. Concerned at a gathering authoritarian surge in many regions, European governments issued Council Conclusions in October 2019 with an upgraded commitment to democracy support\textsuperscript{376}. In 2020, they adopted an Action Plan for Human Rights and Democracy 2020-2024\textsuperscript{377}.

4.1.2. Digital elements in the policy framework

Alongside, and sometimes within the battery of, core external human rights and democracy strategies and instruments, the EU has incrementally accumulated commitments more specifically related to the repressive use of digital tools in third countries.

In 2011, the EU devised its first comprehensive instrument tailored specifically to digital threats to democracy, the so-called ‘No Disconnect Strategy’. This was linked in part to the popular revolts of the Arab spring; while activists’ use of social media revealed the positive democratic potential of digital technology, authoritarian regimes resorted to internet shutdowns and other restrictive moves in an attempt to neutralise the pro-democracy protests that ran through 2011 and 2012. As they did, EU concerns grew that this could jeopardise the Arab spring’s democratic potential and it drew together various parts of its toolbox under the rubric of what it named the ‘No Disconnect Strategy’\textsuperscript{378}.

The Strategy’s strands included funding to help democratic activists build secure communications; training and capacity in cyber security for civil society organisations; and pressure on European companies to step back from abetting Arab regimes’ digital crackdowns, with an attempt to build digital human rights issues into a widened concept of corporate social responsibility. The strategy promised to protect democratic activists and citizens from internet disruptions and surveillance from authoritarian regimes. It proposed funds for projects covering online privacy and security of people living in non-democratic regimes, for educating activists and raising their awareness of the risks involved with online communications, and for building cross-regional co-operation amongst activists to protect human rights\textsuperscript{379}. One concern in the strategy was finding a way to get cyber protection to activists more quickly than allowed for by standard EU tenders and calls for proposals. Under the


\textsuperscript{373} European Commission, ‘\textit{European consensus on development’}, 2017.

\textsuperscript{374} For more detail on these innovations, see F. Gomez, C. Muguruza and J. Wouters (eds.), \textit{EU human rights and democratisation policies: achievements and challenges}, Routledge, London, 2018.

\textsuperscript{375} European External Action Service (EEAS), ‘\textit{A stronger Europe: a global strategy for the European Union’s foreign and security policy’}, 2016.

\textsuperscript{376} Council of the European Union, ‘\textit{Council Conclusions on Democracy’}, 12836/19, 2019.


\textsuperscript{378} European Commission, ‘\textit{Press release: Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally}’, 12 December 2011.

strategy, the EU also moved to prepare a European Capability for Situational Awareness that was designed to provide better information of digital abuses around the world.

While the strategy was an important step forward and innovative for its time, after its key driving force, Commissioner Kroes, retired, some of the momentum behind the No Disconnect Strategy dissipated. The Arab Spring’s atrophy also undercut some of its rationale and the EU had to grapple with complex difficulties in continuing to support democratic reform in this context. At this stage, most Member State governments did not attach priority importance to digital repression elsewhere in the world; they and the top echelons of EU foreign and security policymaking had other geopolitical priorities that cut across the incipient rise in digital authoritarianism. The strategy was soon, in effect, broken up into different parts. While it did not survive in its original forms – like the European Capability for Situational Awareness concept, for example - the ideas it introduced became the basis for the raft of EU instruments that followed in subsequent years.

4.1.3. EU Human Rights Guidelines for Freedom of Expression Online and Offline

In 2014, EU Human Rights Guidelines for Freedom of Expression Online and Offline committed the Union to push back against digital repression. These Guidelines represent a clear statement of intent and an essential part of the EU’s toolbox. They are wide-ranging, but include several commitments relevant to this study. The guidelines stress that ‘all human rights that exist offline must also be protected online, in particular the right to freedom of opinion and expression and the right to privacy.’ These rights ‘must be respected and protected equally online as well as offline’.

In terms of actions, the guidelines are largely about relatively imprecise and soft tools of persuasion, although they do go beyond those of other international organisations in their third-country funding elements. They are mostly couched in terms of promises that the EU will ‘call on states’, ‘appeal to state authorities’, ‘encourage states’, ‘urge states’, ‘ask states for’, ‘advocate against restrictions’, ‘support actions and legislation by third countries’, ‘raise awareness’, ‘condemn abuses’ and ‘facilitate the exchange of experience and good practices’.

Most tangibly, the guidelines say that the EU will ‘continue to provide journalists and other media actors, human rights defenders, political activists and other individuals with the technical tools and support they need in order to exercise their right to freedom of expression online as well as offline’. It will ‘provide technical support to individuals on the ground to help counter online restrictions and abuses’. The EEAS and the European Commission ‘will support the efforts of third countries to develop unhindered and safe access and use of the Internet in the context of ensuring openness and respect for human rights.’

Beyond such concrete funding pledges, the EU will raise restrictions against online freedoms in political dialogues with third countries. Delegations will monitor and report on developments relating to online freedoms around the world, often a difficult task in countries suffering from internet restrictions. The EU promised to ‘encourage and facilitate’ contacts with the CSO on these issues in partner countries. The EU will also monitor and increase its focus on online restrictions in candidate countries through pre-accession processes and mechanisms.

The guidelines contain some more strongly worded intimations at action, like demarches. These state: ‘Abusive restrictions on freedom of expression and violence against journalists and other media actors

---

380 Information in these two paragraphs draw on an interview with representative of an EU institution, 9 December 2020.
should be taken into account by the EU when deciding on possible suspension of cooperation, notably as regards financial assistance’. Many, if not most, of these commitments are hedged with the caveat ‘as appropriate’, which might be read as diluting the EU’s conviction in giving clear priority to this area of concern in its external actions.

4.1.4. Other instruments and initiatives

In recent years, the EU has introduced numerous cybersecurity instruments and initiatives aimed at countering disinformation and other influence operations emanating from third countries; as shown below, these have some points of overlap with the EU’s external democracy support agenda.

The 2013 EU Cyber-security Strategy was mainly framed around a state security narrative, but it also stressed that digital threats to global human rights were relevant to its mandate. The 2014 Council Conclusions on Internet Governance similarly stressed the importance of defending human rights from digital repression.

The new Action Plan for Human Rights and Democracy agreed in 2020 places much greater emphasis on the digital elements to EU external efforts than any previous policy instrument in this field, alongside the standard range of priorities like support for civil society, political parties, and human rights in multilateral forums.

In a recent development, in December 2020, Commissioner Vera Jourova presented the European Democracy Action Plan (EDAP). This is not part of the EU’s external toolbox in the same way as other instruments covered here, as it does not itself entail new funds or diplomatic resources. Yet, it is relevant to this study to the extent that it promises to join together efforts to protect digital rights within the EU with their promotion externally in third countries. The EDAP focuses on three issues: online disinformation, digital attacks on elections, and media pluralism. The EDAP is based on the premise that defending against attacks on elections in the EU and other powers’ use of digital disinformation requires the source of these operations to be targeted within third countries. It points out that this strengthens the need for the EU to support human rights and democratic values internationally. This serves as an important policy reference point for efforts to mitigate digitally-driven authoritarianism globally, even if the EDAP does not in itself (yet) add concrete external funds or foreign policy instruments to the EU toolbox.

Moving beyond this brief sketch of the overarching evolution of EU democracy and human rights commitments, the toolbox can be disaggregated into a number of quite distinctive parts. These include various forms of critical pressure; formal dialogues; funding mechanisms; and the EP’s various instruments. The following sections examine their specific relevance to digital challenges.

4.2. Restrictive measures and conditionality

A first group of EU instruments aims to find ways to exert critical leverage over third countries to improve their democratic and human rights norms. These various instruments are about different forms of pressure over third countries. They have general relevance to human rights and democracy,

385 Ibid.
but also more specific features related to the overtly repressive use of digital tools – they are pertinent, in this way, to a select part of the problematic trends described in Chapter 3, although less so to the more subtle forms of social control or advanced AI techniques.

4.2.1. Democracy and Human Rights Sanctions

The EU has increased its use of sanctions in recent years as its focus on economic statecraft has moved up several gears. It had more than 40 sets of restrictive measures in place at the end of the 2010s. These are mostly restrictive measures targeted against individuals; some are country-based, while others are thematic, as described below. Most of its punitive measures have been related to conflict and security concerns, as in Afghanistan, Bosnia and Herzegovina, Iran, Mali, Russia, Somalia, South Sudan, Syria, and Yemen. Where related to these kinds of conflicts and security concerns, EU restrictive measures are commonly adopted under the umbrella of sanctions agreed in the United Nations. These sanctions are not defined expressly or primarily as human rights or democracy measures, even though in practice they invariably punish human rights abusers involved in violence.

Separately, the EU adopts its own autonomous sanctions. In recent years, the EU has applied such sanctions in relation to human rights abuses and democratic regression. Examples include Belarus, Myanmar, Iran, Venezuela, and Zimbabwe. The EU’s human rights and democracy sanctions have most commonly taken the form of asset freezes and travel bans targeted at a certain number of regime officials, rather than more sweeping measures against a country, per se. The EU generally seeks to retain strands of engagement alongside tightly delineated targeted measures against individuals.

Overall, the EU has generally been relatively sparing in its use of sanctions for democracy and human rights reasons. It has used sanctions often against relatively weak states and where strategic interests were less pressing. It has used restrictive measures in the most serious human rights cases, and it has targeted individuals rather than regime behaviour, as such. Even when the EU has imposed restrictive measures, it has invariably targeted fewer individuals, with softer restrictions and for shorter periods of time, than the U.S. measures in each case. In most cases, the EU has continued to deepen its relations with regimes engaged in digital repression.

EU sanctions could be said to be relevant to digital repression to the extent that the entities and individuals they target come from countries where online abuses have intensified. Digital concerns have been a part of several sanction regimes, including those applied in the cases of Belarus, Myanmar, Iran, Syria, and Venezuela. This was in the form of a listing criterion relating to the use of digital surveillance equipment and prohibitions on the export of monitoring equipment to them.

Still, digital repression has not itself been the main target of restrictive measures nor sufficient as a reason for imposing sanctions. There are many countries where digital abuses have worsened and yet the EU has sought to improve relations rather than sanction such repression; indeed, this is the most common dynamic in EU external action around the world. The EU has rarely sought to separate out digital problems from wider human rights and democracy challenges, as diplomats generally feel this would be somewhat artificial and difficult to do. Its restrictive measures have been applied to cases where online abuses represent just one strand of a far bigger picture of deteriorating political conditions.

387 Interview with representative of an EU institution, 27 November 2020.
In December 2020, the EU adopted a new Global Human Rights Sanctions Regime. This came eight years after the United States introduced the so-called ‘Magnitsky Act’, named after the Russian human rights lawyer Sergei Magnitsky, who was killed in detention. While the new regime is a major step forward, it also exhibits limitations (an analysis of these is beyond this study’s remit but can be found in other sources). How far the new sanctions regime is relevant to digital repression is uncertain. The list of human rights abuses that fall within the mechanism’s scope centres on core issues like torture, killings, violence, slavery, and genocide. The regime excludes corruption as a targetable offense, making it harder to seize kleptocrats’ funds. However, it does include the freedoms of expression and association, which could prove relevant to regimes’ use of digital tools for authoritarian repression (although probably not other elements of the trends outlined in Chapter 3).

Conversely, the EU may now use the new regime to focus more on sanctioning small groups of individuals for egregious rights abuses rather than the more structural and political problem of digitally driven repression. Moreover, the EU’s use of its other sanction regimes in its responses to terrorism, digital attacks on Europe, and the use of chemical weapons could easily cut across the priority it gives to human rights and digital authoritarianism. Good and bad performers are different on these different issues; this means that different sanction regimes could collide with each other and make it more difficult for policymakers to single out issues of digital rights abuses.

4.2.2. Cyber sanctions

More specifically related to the digital sphere, the EU has introduced a sanctions regime against individuals in third countries found guilty of cyberattacks. In July 2020, the first measures were imposed against Russian, Chinese, and North Korean hackers and responsible entities. These sanctions are not directly targeted at digital repression within third-countries, and so their relevance to external human rights and democracy support is not obvious – at least, so far. They are designed to protect the EU itself from digital influence operations; that is, the kind of transnational dynamics outlined in foregoing chapters.

Still, in practice, these are measures against operators within the state apparatuses of regimes that are guilty of particularly far-reaching digital repression. The trolls and other operators in Russia and China penalised for influence operations against the EU – and those that the EU has sought to track more assiduously and effectively by building up its cyber capabilities – are of a piece with these regimes’ digital repression of domestic populations. In this sense, these digital sanctions could be defined as indirect instruments for external human rights and democracy support. The use of these instruments could be widened in this direction, even if for now they are not currently framed in a way that is directly aimed at the global surge in digitally-driven authoritarianism.

The Commission has very loosely and speculatively floated the possibility of developing a sanctions regime specifically for disinformation as part of moves to implement the European Democracy Action Plan, although it is not yet clear whether this will proceed. Whether Member States actually want to make this a top priority is not entirely clear, however. When discussing tougher sanctions and expediting the new cyber sanctions, most EU governments have been reluctant to let digital repression cut across other policy priorities. In a complex episode subject to much internal dispute, uncertainty, claim, and counter-claim, the press reported that the EU diluted its criticism of China’s disinformation

---


389 Council of the European Union, ‘Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States’, 7299/19, 14 May 2019.

campaign during the early months of the COVID-19 pandemic. Stung by widespread criticism, at least some EU commissioners, officials, and leaders seemed to later toughen their position, becoming more critical towards China. The EU’s criticism of Russia for COVID-related disinformation was more robust.

4.2.3. Conditionality

The use of so-called ‘human rights and democratic conditionality’ involves exerting a softer and more subtle form of leverage than sanctions. This does not include legal restrictions or prohibitions, but decisions to hold back funding and/or trade preferences when governments infringe democratic norms or human rights. As with sanctions, the EU has not used such conditionality to such an extent that there is any strong overall correlation between countries’ levels of democracy and EU aid and trade flows.

While the EU often wields a degree of democracy and human rights conditionality, most EU aid goes to non-democratic or partially authoritarian regimes. This general observation applies, with some importance, to the more specific issue of digital repression. The EU often uses its other external funding for aims that sit uneasily with its supposed digital rights commitments. To give just one illustrative example, Chapter 2 identifies India as a state that has used a particularly wide and intrusive range of digital repression and social control mechanisms, and yet the EU has made notable efforts to upgrade its security cooperation with this country for broader strategic reasons. Similarly, China’s even more egregious digital repression has not prevented the EU from deepening its commercial ties or signing a comprehensive agreement on investment with Beijing. Furthermore, in recent years there have been many EU aid projects across Africa and the Middle East, which train security and border guards in how to use invasive digital surveillance equipment, as they work with authoritarian regimes for a range of security objectives.

There is little evidence of the EU using conditionality specifically or explicitly as a response to digital repression or online distortion of democratic processes. The EU most commonly suspends aid for a short period of time following unfree and violent elections, or sometimes in response to very dramatic interruptions of democratic constitutional provisions. So far, political conditionality has not moulded itself to the more specific challenge of regimes using digital repression tools and tactics. In interviews carried out for this study, officials suggested that it would be difficult to separate out specific indicators for digital repression that could, in any primary operational sense, condition the level of overall aid flows to different countries – even if countries loosening restrictive laws could be given specific cooperation to help them do this. Certainly, the more subtle forms of social control, health system development, and AI techniques described previously in this report have not leant themselves readily, or in any tangible sense, to conditionality-based variations in EU levels of cooperation and engagement with third countries. The EU’s monitoring and understanding of digital abuses around the world has improved significantly in the last several years, yet its tangible responses, beyond rhetorical criticism, have not evolved to anything like the same extent.

4.2.4. Restrictions on surveillance equipment

After a crucial and long-running debate that is directly and expressly relevant to the phenomenon of digital repression, in November 2020, trialogue talks resulted in agreeing text for a recast of the dual-use regulation that will tighten restrictions on sales from Europe of digital surveillance equipment to countries where human rights violations are taking place. It is not clear, however, that such restrictions will be severe enough to make these measures an effective part of the EU policy toolbox.

European companies making digital surveillance equipment have grown dramatically in recent years; companies from the EU are responsible for the second-highest earnings from the global market for such equipment. In the early 2010s, some EU states pressed for digital equipment to be included under the multilateral Wassenaar Arrangement on export controls (The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies was established in 1996 and has 42 member states; it works towards ‘promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies’). From as early as 2014, the Commission called for autonomous EU export controls to be extended to digital surveillance equipment.

After several years of internal discussion on this issue, the Commission proposed a comprehensive dual-use regulation in 2016 to tighten controls on the export of potential harmful technology. The core notion was to give the EU the scope to apply autonomous measures beyond the multilateral Wassenaar Arrangement. At this stage, the proposals did not win widespread support among Member States. Member State governments were concerned about how the measures might prejudice security relations with many countries. They were also reluctant to forego lucrative surveillance technology contracts. A majority of Member States worked to dilute the Commission proposals and leave their digital elements relatively modest. For several years, several various Member States undercut the Commission’s efforts to limit EU companies’ exports of digital surveillance equipment likely to harm human rights.

Member States’ opinions began to shift, however, as the scale of digital problems became apparent and also as the United States moved towards far stricter controls, putting pressure on European governments to tighten their own export controls. The use of surveillance against pro-democracy protestors in Hong Kong in 2020 shone a spotlight on digital repression. In this case, the EU did move to prevent companies providing surveillance equipment that could be used against democracy protestors. In 2019, Member States reached an agreement in support of the Commission’s proposals and more constructive negotiations on the details of a new regulation began with the EP playing a vital role as co-legislator.

The Recast Dual-Use Regulation strengthens human rights criteria and explicitly stipulates cybersecurity equipment as a dual-use good. Human rights violations are now a justifiable reason for placing controls on the export of such equipment. The regulation also adds some categories of cybersecurity equipment beyond those already covered by multilateral dual-use controls. There is still much debate over important details within this regulation, particularly relating to exactly what kinds of equipment should be controlled.

---

395 For more detail, see www.wassenaar.org.
397 Interview with key informant interviewee 01, under full anonymity, 24 November 2020.
of equipment shall fall within its remit. Some Member States want a wider scope to include facial recognition technology and other innovations, while others have requested a narrower, more focused approach. Officials acknowledge that compromises have been made and that much will depend on the political will to take the regulation forward. The key factor will be how the EU assesses whether regimes are, in fact, using European technology for repressive ends, and whether such assessments should be made public.  

4.3. Dialogues and multilateral engagement

4.3.1. Human rights dialogues

The EU often stresses the need to exert pressure through political dialogue. It currently has 45 human rights dialogues with partner countries. Formally structured dialogue is a vital part of the EU’s human rights and democracy toolbox. Officials interviewed for this report generally acknowledged that the EU’s human rights dialogues were relatively slow to hone-in on digital concerns, but stressed that they have begun to do so – knowledge and appreciation of the scale of this problem has gradually caught up with trends around the world.

The human rights dialogues that have in recent years come to include a focus on digital rights include those with China, Ethiopia, the Gulf states, and Uzbekistan. In 2021, digital rights and repression will be on the agenda of all EU human rights dialogues. Still, some states have effectively resisted even discussing digital concerns within these dialogues; Russia is a prime example of this.  

The EU approaches its dialogue on digital issues mainly through a freedom of expression prism, although it has begun to include a focus on surveillance and privacy rights. The EU most commonly uses its formal dialogue forums to raise the cases of individuals suffering human rights abuses, including through digital means. The EU has increasingly focused on regimes’ online smear campaigns and repression against opposition leaders and democracy activists. Again, it has also sought to broaden this traditional approach out to address more structural rules that relate to digital rights in third countries.

It is within such external dialogues that the EU has also cautiously begun to expand its digital strategies to address some of the wider array of concerns and controls outlined in Chapter 3. Policymakers are increasingly pushing back within dialogues on states’ use of facial recognition and bio-surveillance, and their use of more subtle techniques, like slowing down connections rather than complete internet shutdowns. They concur that this is where challenges are likely to become pressing in the future, and that much deeper consideration is needed of how the EU can move beyond raising general concerns to making decisions with concrete impact in its foreign policies. Policymakers admit that the EU is still in the early stages of dealing with the international dimensions of AI adoption, which are quite different from the sensitive issues of rights abuses associated with this technology.

In relation to COVID-19 health controls, the EU has increasingly sought to internationalise its focus on data privacy. The EU is now exerting pressure, in both its bilateral dialogues and its interactions with the WHO, to begin discussions on how broader rights issues might be considered in overarching public health diplomacy and policymakers. This is about offering expertise on norm-setting for privacy, but

---


401 Interview with representatives of the EEAS, 2 December 2020.

402 Interview with a representative of EU institution, 12 March 2021.
also looking at forms of pressure as and when regimes use COVID-19 to tighten digital control more broadly over their societies. The February 2021 Council conclusions promising a ‘human rights-based recovery’ from COVID-19 included references to online rights issues, and might serve to help the EU’s incipient efforts to widen the digital components of its human rights dialogues.\(^{403}\) Still, beyond fairly tentative dialogue, most states in the EU are reluctant to use aid that is being disbursed as a humanitarian response to COVID-19 for leverage over a political issue like digital repression.

### 4.3.2. Multilateral dialogue and engagement

Alongside its human rights dialogues with particular third countries or regional groupings, the EU has also increasingly prioritised wider multilateral dialogue for its digital agenda. The EU has promised to strengthen the UN’s focus on and defence of freedom of opinion and expression online, including through the mandate of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, and by cooperating closely with the special rapporteurs with related mandates from the AU, OAS, OSCE and OIC. It has advocated the inclusion of these issues within the Human Rights Council’s Universal Periodic Review process and has engaged with the Office of the United Nations High Commissioner for Human Rights (OHCHR) in relation to online protections.\(^{404}\)

The EU has supported several more specific multilateral forums that are aimed at fostering dialogue on online human rights issues. It has, for example, backed efforts to develop multilateral internet governance forums that protect online rights, like the Internet Governance Forum (IGF)\(^{405}\) and the Freedom Online Coalition (FOC)\(^{406}\). President Emmanuel Macron’s 2018 Paris Call for Trust and Security in Cyberspace stressed that offline rights must also be protected online; it connects 64 states and technology companies with a loose intent to take future action.\(^{407}\) The Commission and High Representative’s proposal for a ‘New EU-US agenda for global change’ presented in December 2020 includes the suggestion that the EU and US set up a ‘Transatlantic Artificial Intelligence Agreement to set a blueprint for regional and global standards aligned with our values’.\(^{408}\)

Most of these forums and initiatives tend to make statements about the need for generic standards, rather than being mobilised in relation to specific cases of rights abuses. It is difficult to identify cases where such dialogue forums have leveraged firm pressure on governments to step back from authoritarian behaviour generally, or the use of digital tools for non-democratic ends more specifically. The EU has struggled to move either the IGF or the FOC beyond dialogue on general standards to become forums that are directly relevant to policy in relation to concrete instances of digital repression.\(^{409}\)

As reported in interviews carried out as part of this study, some policy makers see the current raft of EU measures aimed primarily at regulating platforms’ operations within the Union - such as the Digital Markets Act, Digital Services Act, European Democracy Action Plan and upcoming AI instrument - as tools to be raised more purposively in multilateral human rights dialogues. It is recognised, however,

---


\(^{406}\) See Freedom Online Coalition, available at [www.freedomonlinecoalition.com](http://www.freedomonlinecoalition.com).


\(^{408}\) Commission and High Representative, ‘A new EU-US agenda for global change’, JOIN(2020)22, p.6

\(^{409}\) Garside, p.11
that these generally have a tangential rather than direct relevance to the politics of core global human rights challenges in specific countries. There appears to be an emerging effort to deploy these kinds of new measures to buttress norm-setting at the global level, using their impact on digital questions inside the EU as templates which the EU can use to encourage third countries to implement reforms. Still, the EU is only just beginning to tentatively include discussions on potentially more concrete uses of such instruments for rights-related digital norms in third countries in its human rights dialogues at the global level – a potential step forward, but not one with a tangible impact on the foreign policy toolbox yet. The EU is especially supportive of a UN ‘tech envoy’ with a strong mandate to give these efforts greater impetus.

4.3.3. Engaging the private sector

The EU has worked with the UN to engage the private sector in dialogue about due diligence on human rights. The EU has supported the United Nations Guiding Principles on Business and Human Rights, and worked with the UN to bring digital concerns into national action plans under the rubric of these principles. The Commission has also developed guidance for tech companies based on the UN principles. Still, there are concerns among policymakers that the UN principles are not highly operationally relevant for day-to-day foreign policy challenges and crises, and are not yet an avenue of great potential for a strong approach to tackling the high-level geopolitical tensions involved in digital rights issues. It is also felt that norm-setting related to business and human rights guidelines has been pertinent mainly to the extractive industries sector rather than digital companies, while the new EU human rights due diligence instrument is similarly expected not to be centrally tailored to digital issues.

In its dialogues and outreach, the EU has increasingly sought to persuade private companies to conduct due diligence to ensure their digital operations do not have negative human rights impacts. This is not a new effort, but it is one that has expanded to cover the private sector’s complicity in online right abuses and democratic restrictions. The aim has been to encourage companies to undertake human rights impact assessments and to expand these to digital operations. Several social platforms have commissioned consultancy companies to undertake such assessments. This is not directly part of the EU toolbox, as these are not instruments directly under the EU’s control (such as decisions on funding or sanctions), but the guidance does represent a pertinent means of soft persuasion over the private sector. Those Member States that are part of the FOC have also used this forum as an avenue for dialogue with private sector actors on internet freedoms. At each of these levels, the focus has been on positive encouragement, and there has been little EU appetite to wield punitive sanctions against companies attached to mandatory due diligence requirements.

Policymakers acknowledge that engagement with the private sector is one of the areas where progress has been most modest so far. The EU has gradually begun to redress this situation, although diplomats recognise it is an area that still lags behind the focus on state-to-state relations or the more standard diplomatic channels of foreign policy. The EU has started to arrange several NGO forums with private sector involvement, seeking to position itself as a ‘bridge-builder’ between civil society and private companies. A growing number of such dialogues are focusing on human rights CSOs working with

---


411 Interview with representative of an EU institution, 27 November 2020.


413 Interview with representative of an EU institution, 27 November 2020.
companies to achieve stronger protection of safe online spaces for human rights defenders in autocratic states. Many decision makers believe that the EU is well-positioned to foster this kind of dialogue-based approach with human rights CSOs and businesses, rather than favouring highly punitive approaches, for instance on due diligence (even though on this last issue, some degree of support is growing across different EU institutions and member states for firmer action). Incipient dialogues tend to include social media platforms and aim to get them working with human rights groups. They have not yet aimed to apply concrete pressure on IT companies to actively resist internet shutdowns. Still, notwithstanding these advances, the EU’s contacts, dialogues and coordination with the private sector have so far focused overwhelmingly on internet regulations within Europe itself. Our interviews revealed that the EU has not yet reached out in any concerted way to tech companies in relation to the rights concerns outlined in Chapter 3. There is concern that the spill-over of internal policies into external EU policies has been largely negative; this is because national Member State laws, such as Germany’s NetzDG, have been used by regimes around the world as a template for their own restrictive rules on the internet. Private sector representatives highlight that EU policymakers have been interested in working together to prevent influence operations from third countries having an impact inside Europe, but not to deal with the effects of digital repression within third countries themselves.

As revealed during the interviews, private sector (EU-based and US platform) representatives support the EU’s efforts to develop standards at the multilateral level, but are also concerned that the EU can rather overstate the potential of such guidelines and generic principles. These do not deal with immediate compliance challenges and, in relation to these platforms, some companies do not feel there has been adequate EU diplomatic support, dialogue, or action – often for cross-cutting geopolitical reasons. Since the EU has sought to bring stakeholders together from the private sector, civil society, and governments to coordinate domestic policies, as mentioned earlier, this is gradually being replicated at a broader, international level. One case of untapped potential relates to a possible internationalisation of the Rapid Alert System on which the EU and platforms cooperated for the EU elections in 2019. This kind of coordination is still sporadic in relation to digital manipulation in elections outside Europe, occurring in some countries but not in others, and is not subject to consistent global rules.

4.4. Funding

The EU has gradually increased the funds it allocates directly to democracy and human rights policies. It funds such projects through multiple instruments and budget lines. This makes it impossible to put a single, precise figure on the magnitude of the funding. It is certainly the case, however, that these funds have gained importance within the EU’s overall democracy and human rights toolbox. The EU is currently in the midst of restructuring its funding instruments in ways that will have implications for human rights and democracy generally, and for projects on digital issues more specifically.

4.4.1. European Instrument for Democracy and Human Rights

The budget line that is specifically dedicated to democracy and human rights funding, the European Instrument for Democracy and Human Rights (EIDHR), has amounted to just over EUR 160 million each year since 2014, with a total EUR 1.3 billion for the 2014-2020 budget period. Around 90% of EIDHR funding is allocated for civil society. The EIDHR is a distinctive part of the EU toolbox to the extent

---

414 Interview with representative of an EU institution, 27 November 2020.
415 Interview with private sector representative, 20 January 2021.
that it funds civil society actors without needed formal governmental consent. It can also now also fund non-registered entities, allowing funds to go to a wider range of civic actors, such as those involved in pro-democracy social movements, that can make a significant difference where popular mobilisations have built up strong momentum.

The EIDHR funds the EU’s election observation operations. The EU now deploys some eight to ten election observation missions (EOMs) a year, and an increasing number of electoral follow-up missions (EFMs) \(^{417}\). Of relevance to this report, the EU has recently incorporated a focus on online distortions of election processes in its electoral missions. It did so first in 2018 in Kenya and then in Sri Lanka. The digital remit then expanded and is now formally a part of all EOMs, as well as the electoral expert missions dispatched to more difficult cases where full EOMs are not possible. The EU has worked with the United Nations to develop guidelines on the use of digital technology in elections, with a view to incorporating these into its own missions.

Work on this emerging area of action has been somewhat set back by the COVID-19 pandemic. Election delays and logistical constraints meant that only three EOMs were deployed in 2020 – to Ghana, Peru, and Guyana. Nevertheless, the new Action Plan for Human Rights and Democracy identifies the digital threats to free and fair elections as a top priority for EU external action over the next several years. This action is set to include more rigorous EU monitoring of online activity and tactics during election campaigns, but also more support to build the capacities of local civil society organisations and independent electoral commissions in digital techniques. Officials acknowledge that the main challenge will be to move from a reactive stance of identifying and responding to instances of online electoral manipulation, towards a more pre-emptive policy of preventing such problems emerging well before campaigns begin \(^{418}\).

While the EIDHR is the instrument most directly pertinent to this study, it is important not to overlook the sizeable amounts of funding the EU allocates for democracy and human rights from a range of other geographic and thematic aid budgets. These have included the European Neighbourhood Instrument, the Development Cooperation Instrument, the Instrument of Pre-Accession Assistance, the Instrument contributing to Peace and Security, and various humanitarian aid budget lines. Funding for digital actions has not been an especially high priority in the democracy and human rights initiatives supported under these instruments, but the initiatives have been sources of some additional funds for these issues. Under these, the EU has funded many indirect digital empowerment initiatives that are less overtly political, such as its Digital4Development initiative. The new Neighbourhood, Development, and International Cooperation Instrument (NDICI) introduced under the 2021–2027 Multiannual Financial Framework will combine many of these different sources as a new umbrella framework for the digital elements of democracy and human rights support. With negotiations ongoing at the time of writing, it remains to be seen to what extent the NDICI will prioritise a new round of digital rights initiatives.

From this plethora of different instruments, the EU has focused on several main themes that relate specifically to the challenge of digitally-driven authoritarianism. These are discussed below.

---


418 These two paragraphs on EOMs draw from an interview with key informant interviewee 02, under full anonymity, 26 November 2020.
4.4.2. Media pluralism

Relevant to the digital sphere, media pluralism has increasingly become a priority in repressive environments, and also in countries of conflict, where regimes often use the media to fan the flames of polarisation. This has routinely been framed as part of the EU’s efforts to contain and pushback against non-democratic digital influences. The EIDHR launched a global call on digital activism in 2018, and has identified media freedoms and gender issues as particular priorities for 2019 and beyond. This priority is evident in calls for proposals at the headquarters level, in Delegations’ funding priorities, and in the training currently provided for delegation staff to help them include media pluralism in programming.

European support for media freedom has gained extra momentum from a large-scale Media4Democracy project, allocated EUR 4.3 million in 2017, that focuses on the growing threat to freedom of expression both online and offline. The Media4Democracy project supports EU Delegations to advance several key priorities: combating violence and threats to online freedom of expression; promoting laws and practices that protect freedom of expression; promoting media freedom and pluralism and discouraging interference with impartial and critical reporting; promoting and respecting human rights in cyberspace; and promoting legal amendments and practices to strengthen data protection and privacy. The Commission reports that this initiative has generated an overall increase in Delegations’ support for freedom of expression and media pluralism programmes in the last four years.  

4.4.3. Civil society and digital activism

The EU’s generic focus on civil society support has intensified. Many EU Delegations have agreed on civil society roadmaps. The Commission’s Supporting Democracy initiative provided just under EUR 5 million over three years, sending experts to work with civil society actors and EU Delegations. Through its more flexible funding, the EU has continued to fund some civil society actors even in tough circumstances, such as in Azerbaijan, Belarus, Egypt, and Zimbabwe. This is germane for this report because these are the kinds of states most seriously affected by digital repression. In these contexts, the EU has begun to work harder to enhance societies’ general civic capacity in order to neutralize and offset regimes’ digital tactics. Still, in many of the states identified in Chapter 2 suffering serious digital repression, like China, Iran and Russia, the EU has struggled to keep any significant amounts of independent civil society support going.

Within this broad category of civil society support, in the last several years the EU has begun to focus more on the specific strand of digital activism. EU support for digital civic initiatives has increased significantly in recent years and has become one of the leading edges of the Union’s efforts to counter digitally-driven authoritarian influences. In 2018, the EU ran a CivicTech4Democracy initiative and launched a new EUR 5 million call to support civic activism through digital technologies — “a new priority reflecting the emerging problems associated with the online sphere.” In 2020, the annual, EU-funded NGO Forum was focused on digital challenges to human rights as its central theme. Delegations in Israel and Liberia launched calls on digital democracy in 2020.

419 Online consultation with representative of EU institution, 29 January 2021.
Box 11: EU toolbox on the ground: Myanmar

Even as Myanmar embarked on a tentative political opening from 2012, problems worsened in the digital space. Although Myanmar is a poor country, internet penetration is high, specifically through Facebook. All phones come with Facebook already installed. For several years, the social media space has been used for hate speech and disinformation against minorities, often with at least tacit support from the military. After the military resumed full political control on 1 February 2021, it tightened online restrictions dramatically through a new cybersecurity law, and utilised tactics involving internet shutdowns and severe limitations on freedom of speech.

In recent years, the EU has increased its range of engagement with and in Myanmar. It allocated EUR 600 million in aid under the 2014–2020 budget. The EU has used this budget to fund a rapidly expanding civil society, including for political projects on elections and human rights with digital dimensions. Under a EUR 10 million programme on the elections, the EU supported efforts to increase online transparency around the candidates and their programmes as a way of pushing back against harmful apps. Another programme worth just under EUR 1 million worked to build the capacity of human rights defenders and marginalised groups, including through digital tools and techniques. At the end of 2019, the EIDHR began a EUR 1.8 million initiative to boost online protection for journalists in Myanmar.

At the diplomatic level, the EU has also continued to apply pressure through regular UN Human Rights Council resolutions and through restrictive measures: these have included an arms embargo (that covers dual-use goods and telecommunications equipment), asset freezes, and travel bans on around 40 regime individuals implicated in human rights abuses. The EU has also used the human rights dialogue to try to persuade the regime to change or remove restrictive digital laws. In 2020, the EU decided against removing GSP trade preferences as a means of leverage; the process of ‘enhanced engagement’ raised gross human rights and labour rights violations, although it did not identify digital restrictions as such. The military’s move in 2021 to resume direct, fully autocratic control revealed the limitations of these various strands of engagement and left the future of EU projects on the ground uncertain.

4.4.4. Protecting activists from repression

Arguably most relevant to this report’s remit is that more of the EU’s funding now goes directly to protecting activists from state repression. Increasingly, “EU democracy support has shifted towards pushing back against negative trends like the shrinking space for civil society, disinformation, and attacks on electoral integrity”424. This funding has evolved in response to what Chapter 3 refers to as the ‘next generation toolkit’ of digital control. The EIDHR’s emergency fund for human rights defenders can directly channel funds at speed when defenders face a moment of acute risk425.

The EIDHR also funds a human rights defenders’ protection mechanism, known as Protectdefenders.eu. ProtectDefenders.eu was set up in 2015 in order to provide a more comprehensive direct support mechanism for human rights defenders. It includes training on digital security for online activists, as well as temporary relocation and support for judicial procedures. Under this project, a consortium of

---


425 Ibid.
12 international NGOs provide emergency grants for relocation, individual security, and legal support. By early 2019, Protectdefenders.eu had provided over 1,000 emergency grants, training for 5,000 at-risk human rights defenders, and other support for just over 10,000 human rights defenders. The EU has recently extended the contract until 2022 for the amount of EUR 10 million. The extent of digital protection, equipment, and training provided under the EU's various emergency grants has increased significantly in recent years. It is set to rise further as a priority under (the fourth pillar) the new Action Plan for Human Rights and Democracy from 2020 onwards. The Commission has encouraged Delegations to fund digital initiatives as a horizontal priority under human rights and democracy funding as a whole (especially the thematic programme that will secede the EIDHR) and to increase the scale of digital training for human rights defenders and journalists.

4.4.5. European Endowment for Democracy

Finally, one additional actor warrants mention. In 2013, a novel addition to European democracy funding began work: the European Endowment for Democracy (EED). The EED functions outside the formal EU institutional structures, although it is funded by the Commission and Member States. Since 2013, the EED has funded over 1,000 projects, worth more than EUR 50 million. 23 Member States have contributed funds. Initially, it worked only in European Neighbourhood Policy states, but in the latter part of the decade it has expanded to Russia, Turkey, and the Balkans. The EED's budget is still relatively small, at under EUR 20 million per year, but the organisation has established a high profile within European democracy support.

The EED follows ‘an unconventional approach to democracy support’ designed to fund democratic activists that do not receive help from other donors. It has flexible administrative rules that make it easier to support small, informal, or non-registered organisations; or even individuals. It funds new types of activism. The EED has a particularly strong focus on citizen journalists and grassroots organisations working to pushback against digital repression; digital literacy; alternative content generation; capacity-building for local digital initiatives; digital security for activists; and tailored protection for individual bloggers attacked by regimes.

---

426 Ibid.
427 Online consultation with representative of EU institution, 29 January 2021.
429 Interview with a representative of the European Endowment for Democracy, 22 December 2020.
Box 12: EU toolbox on the ground: Kyrgyzstan

On the ground in individual countries, EU diplomats face the challenge of dealing with digital and human rights issues as part of a wider ranging agenda. A case like Kyrgyzstan shows how, in practice, different parts of the EU toolbox interact and overlap with each other. This is a country where the digital agenda is relatively new for the EU and is just beginning to gather momentum, but where it has clearly grown in importance in recent years. The country is an example of a hybrid regime with some reformist elements, but an overarching trend of democratic backsliding. Neighbouring powers like China and Russia are distorting discourses and communication on the internet, but also some internal actors. Within this context, the EU has built digital components into most of its policy instruments. In terms of funding, the Media4democracy initiative has paid for civil society training. The EU has supported a EUR 21 million programme for digitalisation that is not specifically concerned with human rights, but includes some policy dialogue on rights standards. Digital concerns have become more of a priority within the EU's human rights dialogue; the EU teamed up with the UN to convince the government to pull back from a number of restrictive digital laws. The EU is also providing additional support to human rights defenders hit by digital attacks. It is building digital issues into a new, enhanced cooperation agreement set to come into effect next year, some focusing on online rights. It seeks to use the leverage of GSP-plus for the same aim. New post-2020 aid will include more work on digitalisation. The EU is beginning to develop all of these means of leverage, even though digital restrictions cannot yet be defined as one of the highest priorities. This case shows that on the ground, the digital element is one issue nested within a range of other political trends, and so it cannot be separated from these. The EU has deployed a combination of dialogue, funding, and pressure, grappling with the challenge of a context that allows some cooperation on digital tools, but where political trends continue in a negative direction despite the EU's upgraded efforts.

4.5. Overlaps with cyber-security and influence operations

The EU has developed a cluster of instruments in recent years that aim to strengthen the Union’s ability to withstand various types of digital influence operations from third countries. This is a different agenda to support for human rights and democracy within third countries, which this report covers. Nevertheless, these two agendas have begun to overlap in places. A number of the new and emerging instruments in this area have begun to develop in a way that are relevant, at last at the margins, to this report’s subject matter.

4.5.1. Stratcom

One very politically driven area of external funding activity has been carried out under the so-called Stratcom initiative, set up in 2015 by the External Action Service. With a very specific remit to counter Russian disinformation in the countries of Eastern Europe, the initiative worked to correct Russian disinformation and contribute to spreading good news stories about the EU in these countries. In this sense, the initiative has indirect relevance to this report’s concern with digitally-driven repression in third countries. Stratcom was mobilised as a tool mainly to protect against disinformation within the EU and some non-EU Eastern Partnership states; it followed a security agenda, rather than aiming directly at human rights and democracy within the source countries of disinformation.

---

This box draws from an interview with a representative of EU institution, 15 December 2020.
Still, the lines between these two agendas have been somewhat blurred. Stratcom’s budget increased from EUR 1.1 million in 2018 to 5 million in 2019, and its remit was extended into the Balkans, North Africa, and the Middle East. Of direct relevance to this report, Stratcom operations in the south and the Balkans focus more on building local capacities to resist digital distortions to democratic processes and disinformation, in particular, than they have done in the east.431

4.5.2. Cyber funding

In recent years, the EU put in place a large number of initiatives in the realm of cybersecurity. While these are designed to protect the EU’s security from outside influence operations, a number of the new initiatives in this field have taken on at least some elements related to digital repression in third countries.

An initial EU Cybersecurity Strategy in 2013 was designed mainly to draw together the large number of fragmented areas of cybersecurity work in the EU, and better connect these to foreign policy. The Cybersecurity Emergency Response Team initiative was one of the largest projects funded under PESCO, while the European Cybersecurity Research and Competence Centre also gained influence. In 2017, the EU introduced the Cyber Diplomacy Toolbox. The issue was ostensibly mainstreamed into core defence policy through the 2014 Cyber Defence Policy Framework; this was updated and significantly expanded in 2018. Overall EU spending on cybersecurity increased exponentially, equating to billions by the end of the 2010s.432

The EU Agency for Network Information Security (ENISA) morphed into a more institutionalised Agency for Cybersecurity, gaining powers and resources. In 2019, its budget doubled from around EUR 10 million to over EUR 20 million per year. The EU agreed a framework for a Joint EU Diplomatic Response to Malicious Cyber Activities. By 2019, cybersecurity accounted for half the workload of the Security Union.433 The EU introduced cybersecurity dialogues into all of its main strategic partnerships and, in 2018, the High Representative convened a Global Tech Panel to examine the geostrategic implications of digital technology.

It also set up a hybrid fusion cell and the European Centre of Excellence for Countering Hybrid Threats; agreed an action plan against disinformation; set up a 24/7 rapid alert system for Member States to notify of foreign disinformation campaigns; and got the major online platforms to sign a code of practice to cooperate on tackling disinformation. G7 leaders agreed to the so-called Charlevoix Commitment on Defending Democracy from Foreign Threats, committing to take concerted action to respond to outside threats to democratic elections. The EU’s 2020 Cybersecurity strategy then promised further to tighten the link between digital security issues and mainstream foreign and security policy strategies.434

Concerns around cyberattacks within the EU led to the allocation of funds for digital security initiatives in third countries, as a way of boosting their cyber resilience. Under the Instrument contributing to Stability and Peace, the EU is funding an increasing number of cybersecurity projects in other countries. While cyber funding has been primarily aimed at boosting cybersecurity capabilities within the EU, its external component has begun to expand.435 This strand of policy is mentioned here because it is becoming an increasingly high priority for the EU; it has yet to incorporate any significant funding.

431 Interview with representatives of EU institution, 27 November 2020.

432 European Court of Auditors, ‘Challenges to effective EU cybersecurity policy’, Briefing paper, 2019.


434 European Commission, The EU’s cybersecurity strategy for the digital decade, JOIN (2020) 18 final

directly targeted at digital authoritarianism as such, although these capabilities could *de facto* prove highly useful in protecting civil society activists from attacks.

4.6. Possible responses to Pegasus and equivalent surveillance spyware

4.6.1. How has the EU toolbox dealt with spyware?

In addition to all these policy responses to the general challenge of digital authoritarianism, the EU has been obliged to grapple with the external-policy dimensions of Pegasus and other spyware challenges. Understandably, much focus has been on the use of this spyware within EU member states and the operations of EU companies, as a matter of domestic policy. Much critical focus has been on civil society organizations’ allegations of member state governments using it to spy on opposition figures: most controversially in Poland, Hungary, Spain, and also Germany, Belgium and the Netherlands. There is a need for the EU to strengthen internal rights and privacy protection in response to these cases, and on whether there can be any genuine security-related government use of Pegasus.436

While these domestic dimensions have understandably dominated debate, they are beyond this report’s remit. The Pegasus issue has opened a number of foreign policy dilemmas too. The EU needs to work to limit the global use of spyware, not just within its own borders. Confronted with this more specific part of the digital agenda, the EU toolbox is less developed in this area and is still adjusting to the magnitude of threats posed by latest-generation spyware, as detailed in section 2.6 above.

Several types or levels of external-policy challenge can be distinguished from each other in this area. It is important to stress that the foreign policy aspects are not only about trade of spyware into and out of the EU itself but also involve other more political aspects too. There are a growing number of examples of third-country governments using Pegasus and other spyware against EU citizens, politicians or officials. The Moroccan government has reportedly used it against Spanish and Belgian politicians and journalists. The Rwandan government has used it against Belgian journalists. These examples invite some kind of EU reflection and response as they directly involve EU citizens.

Regimes around the world are using spyware against their own citizens, opposition forces and human rights activists, as detailed in chapter above. This compounds the existing arsenal of digital repression that regimes are using to curtail personal freedoms and civil liberties. As the EU has ratcheted up its commitments to defend such basic democratic and human rights, this directly repressive use of spyware will need to be incorporated into the core elements of EU democracy and human rights support. Spyware is being used against and to the detriment of the very civil society leaders and organisations that the EU is funding, and in this way undoing the impact and value of such European support.

In some cases, EU countries are themselves the source of latest-generation spyware being exported around the world, including in some cases to regimes with highly undemocratic features. As outlined above, the EU has been debating its rules for curtailing or conditioning sales of surveillance equipment over the course of many years. The emergence of the latest generation of and advances in spyware presents a further element of this debate. It will be more difficult for the EU to meet its external policy objective of limiting other countries’ use of spyware and the general global reach of such intrusive technology if European companies are themselves adding to this supply and the spread of repressive technology.

---

The general EU policy framework outlined above has not yet fully caught up with these external dimensions of the spyware threat. The series of guidelines and principles laid out in existing EU documents and strategies are generic enough to cover many of the effects of spyware. The use of spyware clearly falls under the kind of broad digital repression identified by these general policy frameworks. In this sense, the existing set of existing policy commitments should facilitate EU responses to this growing problem. Indeed, they would seem to call for or even oblige a more assertive and systemically pursued EU policy towards spyware.

Still, as this problem becomes more widespread the existing policy framework needs updating to incorporate more specific guidelines, commitments and indicators that speak to the spread of spyware.

4.6.2. Sanctions

If the EU’s sanctions regimes on human rights and cyber-attacks have so far had a relatively modest relevance to digital repression, they have had even less prominence in relation to spyware. In formal terms, the global human rights sanctions regime could certainly be deployed, as regimes’ use of spyware infringes some of the core individual rights named as motive for EU action. However, the EU seems to be tilting towards a sparing use of this sanction regime. No individuals have been added to the listings in 2022, to date. With so many egregious human rights abuses around the world not being targeted under the EU sanction regime, it does not seem that the specific issue of spyware is set to be a prominent part of discussions.

Nor is it clear that spyware concerns dovetail well with the EU cyber sanction regime. Countries’ authorization of spyware use against EU citizens and politicians does not fall into the same category as direct cyber-attacks on infrastructure and the like, of the kind that this sanctions regime has targeted. The EU has also used this sanction regime sparingly and caution appears to prevail over the possibility of its wider use. The cyber sanction regime would need to be widened explicitly to specify instances where third-country governments use spyware against EU citizens or officials in member state authorities or EU institutions. This could offer a tailored way forward, although to date most member states have steered away from such punitive approaches.

4.6.3. Regulating trade in spyware

The Recast Dual Use Regulation is clearly relevant to stopping spyware made in EU states being exported. This regulation could be updated to build in specific provisions in relation to this, but member states have not yet advanced in this direction. The European Data Protection Supervisor has called for such an update of the regulation expressly to cover these products. This update could be framed to ensure spyware products are sold in accordance with human rights standards and also to ensure that they are imports into EU states only from states employing human rights criteria. When corporate entities linked to NSO in Cyprus and Bulgaria were suspected of having re-exported Pegasus, the EU did bear down on this. As of yet, however, the EU has not yet moved to build anything specific on spyware within the conditions governing its licensing decisions.

The EU-US Trade and Technology Council has begun to discuss these kinds of issues in more detail and is seen as a possible forum for future progress. Still, since February 2022 the EU’s policy attention and institutional capacities in relation to dual-use technology export restrictions have understandably been targeted at Russia sanctions related to the war in Ukraine. Moreover, so far, policy considerations have been on exports, with little focus on any mirror provisions relevant to imports.

There is a growing debate about use of new due diligence rules, in order to push vendors to do their due diligence and not sell to governments with poor human rights record. This focus on due diligence is an increasingly dynamic area of EU policy development and could potentially open the door to limit
spyware trade flows. Policymakers acknowledge that so far the range of instruments relevant to this issue – including the EU’s upcoming due diligence framework, OECD due diligence guidance for responsible business conduct, EU corporate sustainability reporting – have not homed in on spyware related rights concerns, as their focus has been on more standard and egregious right issues like forced labour. Debates are unfolding about how far the tool of due diligence might be stretched – how wide a range of rights issues might be included – without targeted impact being lost. A potential due-diligence link is where spyware might be associated with the use of forced labour in third countries.

The section above shows how the EU has struggled to push the private sector to engage with digital repression in third countries. The expansion of the spyware challenge increases the need for it to do so. The EU could work with companies specifically to identify how spyware could affect their own operations and develop guidelines to ensure that EU companies raise abuses linked to spyware use.

The most stringent option would be to introduce a ban on the export from and import to the EU of any spyware, at least for a defined period of time while the EU works out robust principles to govern its use. If member state governments do not support this, the next most ambitious option would be to introduce a rule that EU companies can only export spyware to democratic countries with strong human rights records. On the import side, the EU could also ban sales into the EU from non-democratic states. There has not been member state support for really tough or high-profile responses and these kinds of options have not been discussed with any serious intent. The EU has not contemplated the kind of entity list that exists in the US as a means to blacklist defined companies, and there remains a relative lack of transparency on these sensitive trade related debates within European decision-making.

4.6.4. The Wassenaar Arrangement

The Wassenaar Arrangement was established in 1996 as a voluntary export control regime comprised of 42 countries. Most of the membership is made up of democracies, but there are outliers; Russia and Turkey, for example, are members of the organization. Members exchange information about the transfer of conventional weapons and dual-use goods. In 2013, members agreed to add two types of dual-use technology for regulation: intrusion software and IP network communications surveillance systems. The implication of this regulation was to obligate members to exchange information on all export licenses issued or transferred to non-Wassenaar members and to notify the Wassenaar Secretariate of any export licenses denied on proposed transfers to non-Wassenaar members. The 2013 rule faced significant criticism from industry and civil society, who argued that it contained vague definitions about what constituted “intrusion software” and would restrict legitimate tools needed for security research and cyber defence.

At the December 2017 meeting of the Wassenaar Arrangement, the United States sought to “correct” overly broad controls on intrusion surveillance software that experts claimed “criminalized” legitimate tools for stopping malware. They argued that the entries were overly broad, capturing more than was intended, and as a technical matter, failed to accurately describe the items intended for control. In addition, many commenters asserted that the controls imposed a heavy and unnecessary licensing burden on legitimate transactions that contribute to cybersecurity. Members agreed to incorporate changes to the 2013 text. Based on the understanding reached in 2017, the Commerce Department announced a new rule in late 2021 that aligns U.S. policy with other members of the Wassenaar

---

437 Arms Control Association (2022), The Wassenaar Arrangement at a Glance
438 Decipher (2021), U.S. Export Controls Crack Down On Surveillance Tools
439 Lawfare (2018), Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research
Arrangement. The new rule limits the export of malicious software to authoritarian countries while not preventing American researchers from detecting software vulnerabilities or stopping cybersecurity firms from responding to incidents. It would prohibit sales of hacking software and equipment to China and Russia, as well as to other countries of concern, without a license from Commerce. The rule would also apply to commercial intrusion software, such as Pegasus.

While the United States has helped resolve a problematic aspect to Wassenaar’s dual use controls, Wassenaar continues to exhibit significant weaknesses when it comes to limiting spyware exports:

- Members are free to choose whether to enact controls on listed items and whether to enforce any enacted controls. Just because a country is a member of Wassenaar does not mean it is bound to take any action at all, rendering Wassenaar little more “than an organization for sharing information about export controls without the institutional teeth to actually control exports”.

- In early years, a few members “consistently refused to fully participate in voluntary information exchanges and notifications on dual-use goods”. Reportedly, participation has improved, but the voluntary aspect of Wassenaar indicates a structural weakness.

- There is little consensus among members about which countries are "states of concern" which would entail preventing such states from acquiring sensitive dual use goods and technologies. There is also no consensus about what constitutes a “destabilizing” transfer.

- Several major arms exporters, including China, Israel, and Belarus, are not members of Wassenaar, thereby opening a significant export controls loophole.

- While Wassenaar limits the export of sensitive dual use goods and technologies to non-members, it does not prohibit the purchase of surveillance technology from a non-member. The import of Pegasus spyware to EU states demonstrates the weakness of this provision.

4.6.5. Diplomatic relations

Trade restrictions would only address one modest part of the external dimensions addressed in this report. The geopolitical dimension of spyware is not only about export-import flows directly involving EU providers or buyers. The external dimensions of the spyware challenge go far wider. Even a complete EU trade ban on spyware would not comprehensively address the use of spyware in third countries as a leading tool of autocratic control. Nor would it stop third-country governments using spyware against EU citizens from outside Europe. While much attention has been directed at regulating private sector activities, the EU also needs to decide whether it is willing to attach high priority to spyware concerns through it standard diplomatic relations.

A focus on export rules is needed but would only grapple with one part of the problem. Most trade flows in spyware involve transfers between different third countries outside the EU. EU dual-use trade rules do not speak to the dilemma of spyware being supplied from one third country to another third country, for instance. EU governments cannot simply push this onto companies, pressuring them not

440 Department of Commerce, Bureau of Industry and Security 15 CFR Parts 740, 772, and 774, Information Security Controls: Cybersecurity Items


442 Arms Control Association (2022), The Wassenaar Arrangement at a Glance

443 U.S. Department of State (2000), Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Fact Sheet Released by the Bureau of Nonproliferation
to deal with these non-democratic regimes with which the EU and member states governments maintain friendly security relations.

The EU has still not determined that it attaches sufficient priority to this problem to incorporate it into mainstream diplomatic relations. Policymakers acknowledge that one challenge is that core EU legal and policy frameworks relating to human rights do not offer precise reference points to be used in relation to spyware: spyware issues related to rights infringements are not yet codified in the same way as longer-standing human rights issues, making it more of a political step for diplomats to foreground them in diplomatic processes. Spyware issues are not yet enshrined with explicit precision within EU or member state foreign policy and security strategies.

Debates over pressuring governments in relation to spyware usage have been low profile. When the Moroccan government was accused of using Pegasus on Spanish politicians, the Spanish government did not react with any measures as it sought to maintain fledgling deepened cooperation on migration and border control from the Moroccan regime. The EU has endeavoured not to let its security cooperation with several other Arab regimes be derailed by their use of spyware against civil society and opposition figures. The EU has sought to revive trade talks with the Thai government despite its use of spyware against democracy activists. Some of the main exporters of spyware include EU allies like the US, Canada, South Korea, the UK and Switzerland, as highlighted in chapter 2.

This is, of course, challenging as the EU has a wide range of other interests and concerns. But it could begin to insist on critical dialogue with partners around spyware within its existing toolbox of human rights dialogues, outlined above. One avenue that diplomats are beginning to explore relates to the EU’s Guidelines for Human Rights Defenders. The EU has recently included reference to these applying to digital techniques being used against human rights defenders, including those techniques associated with spyware. These are not legally codified provisions, but the Guidelines do seem set to become a political tool of potential relevance to the spyware challenge where regimes use spyware specifically against human rights defenders.

The EU has not adopted measures against the NSO Group or similar commercial spyware vendors but could find ways to do so. NSO insists it respects UN principles on Business and Human Rights and has moved to cut off supplies where there is misuse and has refused to sell to a large number of governments with bad human rights records. Yet, concerns remain. While the US put NSO on its entity list – causing it serious difficulties - the EU has declined to take such a step.

---

444 Politico (2022), EU spyware inquiry fails to put Spain on list of fact-finding trips
Box 13: EU relations with Israel in the light of Pegasus case

These dilemmas have particular relevance to EU relations with Israel given its central role in the latest wave of spyware problems. Debate over sanctions towards Israel is a perennial feature of internal EU foreign-policy debates, and generally an inconclusive one as unanimity is commonly absent when possible punitive measures are raised in relation to Israeli actions. There have been so many calls over so many years for the EU to take tougher measures against Israel in relation to its actions against the Palestinians; the EU has adopted only very modest measures like excluding Israel from some EU funding programmes. If anything, Israel has imposed more severe conditionality on the EU, excluding it from any leading role in peace-process diplomacy. As long as the EU declines to take punitive measures on Israel for actions that lead to Palestinian deaths and flout international law on settlements, it is difficult to see that the authorizing spyware exports is likely to attract EU sanctions.

At present, the EU focus is on repairing the EU-Israeli relationship after some difficult years. In September 2022, an EU-Israeli association council was held – the first since Israel pulled out of these in 2013. The priority is to bring a two-state solution back into play, while Israel has also become more important for EU energy security. The EU appears reluctant to put these wider strategic aims at risk by focusing on spyware concerns in any punitive fashion. The Commission says it has raised concerns with Israeli authorities; the EP has been pressing for more details and information on what concrete steps will be taken. Yet, far from the EU imposing any punitive measures on Israel in relation to Pegasus concerns, policy seems to be moving in the opposite direction towards a new rapprochement.

Against this backdrop, the question is whether the EU might use its toolbox for more targeted pressure. The Israeli government insists it authorizes exports of Pegasus only to governments to tackle crime and terrorism and points out that it has reduced its authorized cyber export list as concerns have grown about the spyware, from 102 to 37 countries. Yet the EU could push for Israel to join the Wassenaar Agreement and employ formal human rights criteria in its spyware authorisation decisions (it has adopted the Wassenaar list of dual-use items subject to control).

For the moment, the EU has so many challenging issues on the agenda with Israel, it has not expended significant political capital on the Pegasus issue in this relationship.

### 4.6.6. Funding

A final strand of the EU toolbox relates to funding in third countries. The section above details the various strands of EU democracy and human rights funding, and outlines how they have begun to deal with issues related to digital repression. These funding instruments have not yet caught up with the challenges presented by the latest wave of intrusive spyware. The initial and most basic concern has been to ensure that EU funding does not actually facilitate the use of spyware as part of security cooperation programmes in third countries.

Several funding streams could implement specific funding calls and initiatives to target the spyware problem. This would represent a relatively indirect and bottom-up approach that might prove helpful over the long-term. EU funds could support civil society organisations to monitor the use of spyware in third countries and to critically engage against this use where it infringes human rights and democratic standards. Change is beginning to happen, policymakers say, with EU funding initiatives supplying increasing amounts of general digital security equipment to civil society organisations that has a read-

---

over to the spyware challenge. While policy discussions on this remain embryonic for now, from the NDICI instrument to the EU’s various emergency grants and the EED, there are several possible parts of the existing toolbox that could be used for such an approach.

4.7. **EP instruments and contributions**

Through its Democracy Support and Election Coordination Group, the EP increased its work from 2014, mainly in the form of election observation and exchanges with other parliaments. Its activities include actions around the Sakharov prize, concrete capacity building, mediation, and support to human rights defenders and journalists. Some of these tools are relevant to new challenges in the digital sphere. The group lists countering fake news and supporting media pluralism among its priorities. Its 2020 work programme does not foreground digital issues. Rather, it lays out the geographical priorities for its fact-finding missions and (pre- and post-) electoral dialogues, and for its large number of training, young leaders, fellowship, and human-rights related awards programmes. Still, it contains one highly significant mention of digital issues; the EP offered to co-host a meeting with the EEAS to support the latter’s efforts to develop a ‘declaration of principles for international election observation’ that would include digital technology concerns.

More broadly, the EP has worked to raise the profile of several areas of digital issues and their links with human rights and democracy. In 2012, the EP passed a resolution entitled ‘Digital Freedom Strategy in EU Foreign Policy’ that urged the EU to place higher priority on defending ‘digital freedoms’, in particular within its development and other external funding programmes. In 2015, it passed a resolution on ‘Human rights and technology: The impact of intrusion and surveillance systems on human rights in third countries’. This focused primarily on concerns that the EU had failed to prevent European companies from supplying digital surveillance equipment to third countries that do not have rigorous human rights assessments. It also called for a number of concrete steps relating to the external promotion of digital rights. These included a ‘human rights and technology fund’ to be created under the EIDHR; new clauses to be included in all trade agreements referring specifically to the need to respect ‘digital freedoms’ and unhindered access to the internet; and a ban on companies failing to apply the digital due diligence elements of the UN Guiding Principles on Business and Human Rights from EU public procurement calls. The interviewees for this study concurred that these EP resolutions have played a role in pushing the Commission and the Council to take action.

In the last several years, the EP has played a prominent role as co-legislator in relation to tightening export controls on dual-use surveillance equipment in line with the Commission’s Recast Dual-Use Regulation. The DROI Subcommittee on Human Rights heard evidence in 2020 on COVID-19 related disinformation. The European Parliament has put in place a special committee on ‘Foreign Interference in all Democratic Processes in the European Union including Disinformation’. While this is focused on policy concerns within the EU, its Rapporteur’s first working documents make several references to the need to connect this concern with more active external action directed at digital abuses.

---

446 Democracy Support and Election Coordination Group.
4.8. Conclusions - assessment of the toolbox’s evolution

The EP’s 2015 study, mentioned above, was not a detailed study of all elements of the EU toolbox or specifically of the external dimension of digital rights issues, but it did suggest some general steps forward. These have proven highly relevant to subsequent policy developments, as the EU has moved to take on board nearly all of the report’s main suggestions, namely: to ‘encourage’ other countries to respect digital freedoms; to build institutional knowledge on such issues; to bring digital issues into external dialogues (singling out Latin America in this regard); to make cyber-security more about rights and less about purely military-type security approaches; to support online protections for citizens outside of Europe; and to push for more UN work on digital privacy. As this chapter has demonstrated, the EU’s policy toolbox today reflects all of these ideas to a far greater extent than was the case before 2015. However, in the last several years, more specific issues have arisen in the EU’s deployment of its toolbox that raise further challenges for the EU to address and continue improving its policy instruments. New concerns have arisen over the effectiveness, comprehensiveness, and efficiency of the EU toolbox, while various thematic dilemmas have become more acute:

Effectiveness: In recent years, the EU has retained – and even widened – its toolbox for human rights and democracy support against an extremely challenging global backdrop. Yet, the challenge of digitally-led authoritarianism has continued to deepen. As a result, the EU will need to look for ways to continue fine-tuning and adding to this toolbox. While the EU’s general approach to human rights and democracy has sharpened in some notable ways, it is more difficult to conclude that its toolbox is fully attuned to the specific features of digital repression and contemporary democratic backsliding.

The EU’s direct financial support has had a very clear, tangible impact on protecting many individual civil society activists from repression. Its broader funding initiatives aimed at enhancing the positive digital capacities of civil society have been useful in laying the groundwork for pushing back against digital repression, but the impact here is almost impossible to quantify with any precision. The EU’s diplomatic pressure, dialogues, and attempts to build effective international standards are areas where the interviewees in this study felt that the EU’s effectiveness is the hardest to pin down, in terms of an identifiable impact on the regimes’ immediate political actions. While EU policies have improved, the desired results have not always been forthcoming, as regime attacks on democratic freedoms and human rights have become stronger and more far-reaching.

Comprehensiveness: The EU’s toolbox has become more comprehensive in the last several years, as the EU has added a number of different strands to its efforts against digital authoritarianism. Digital rights issues have been incorporated, to some extent, into EU restrictive measures. Funding has increased for digital elements of external human rights and democracy. Online threats to democracy have become a staple of EU dialogues with third countries and within multilateral fora. EU cybersecurity cooperation has begun to adopt more of a rights-centred approach. Alongside focusing on regimes’ repressive actions, the EU has also moved to limit European companies’ involvement in supplying digital surveillance equipment, and to persuade ICT companies to ensure they do not contribute to digital authoritarianism. Its moves in relation to Hong Kong provide the most significant, concrete example of this. Considered as a whole, these actions constitute a more multi-pronged approach than was apparent earlier in the 2010s. Still, it is clear that the EU toolbox does not yet fully cover all digital challenges, and that some of the emerging techniques of social control, health-system management,
and advanced AI described in previous chapters have not leant themselves easily to EU foreign policy tools, and are only just beginning to be included in EU external dialogues.

**Efficiency:** The EU has made some impacts on a relatively low-cost basis. While it has invested increasing amounts of money in digital initiatives in third countries, funding in this area is still relatively modest. There remains scope for the EU to significantly ramp up the promising work it has embarked upon through digital funding programmes in recent years. To date, the EU has not been willing to incur significant costs in terms of letting trends in digital repression impact on its commercial and strategic interests. It will need to consider more carefully whether this caution might result in higher ‘costs’ in the longer term.

**Sanctions and conditionality:** While the EU has fine-tuned its use of restrictive measures related to democracy and human rights, it remains uncertain how relevant these are in response to the digital aspects of repression and rights abuses – as opposed to coups, stolen elections and egregious human rights abuses in violent contexts, where the EU has been more likely to impose sanctions. The EU has become better at monitoring online problems, but it is often difficult to separate these out from other policy concerns in terms of on-the-ground responses.

The EU’s new cyber sanctions regime could mark a significant change in this regard. For now, however, this is designed to respond to digital influence operations against the EU, rather than digital forms of authoritarian control within third countries – even if, in practice, there is overlap between these two phenomena. The EU’s new Global Human Rights Sanctions regime will target individuals, entities, and bodies. Still, this may not be an instrument relevant to the more structural or institutional levels of states’ digital repression, which extend far beyond the actions of a few individuals or entities.

**Resources:** Resources still need to be increased if the EU is to make any significant headway against digital repression. Despite funding increases, funds for democracy and human rights have been limited, relative to other areas of EU spending. The EIDHR has been the smallest of all EU funding instruments, and the EU’s other funding instruments have remained rather under-utilised for human rights and democracy in general, and for digital elements of this agenda in particular.

EU external funding has supported an increasing number of digital rights initiatives. Still, there remains considerable scope to increase these allocations to make digital issues a clearer priority element of external democracy and human rights support. There are countries suffering especially severe digital repression in places, where this part of the EU’s toolbox has not yet proven relevant. China is a notable omission from digital funding profiles, as any kind of civil society support there has become extremely difficult. While the EU’s new 2021–2027 budget includes a modest increase in human rights and democracy funds, it is too early to ascertain the extent to which the new streamlined funding instruments will focus on digital repression. Some interviewees expressed concern that the new multiannual financial framework (MFF) appears to accord greater priority to security and migration issues, raising the perennial question of inter-issue trade-offs.

**Digital distortion in elections:** The EU’s tentative moves to build digital considerations into its electoral missions are an important step forward, but will need to be expanded to other countries and benefit from higher resource levels and political backing if it is to have significant impact. It would be valuable to use this change as a base from which the EU can link together its electoral work with long-term capacity building on digital empowerment within civil society and other instruments. EU policymakers have long recognised the need to make stronger connections between electoral missions and other elements of democracy support; the rise in digital campaigning and online distortion to democratic processes make this an even more urgent imperative.
Gradual democratic backsliding: A more general shortcoming comes from the fact that digital repression can often be subtle and accumulate incrementally. The EU tends to clearly react to dramatic interruptions of constitutional processes and obviously manipulated elections, but struggles to respond to these more gradual threats. Many regimes that are not fully authoritarian are assertive users of digital control tactics, yet these are the kind of regimes that the EU has sought to engage for other policy aims, neglecting to foreground the insidious impact of such digital repression.

Technocratic governance focus: The EU still also needs to grasp the highly political nature of digitally-driven challenges to democracy and human rights. A lot of European funding has been relatively technical in nature, as it has focused on state institutions. Most EU political aid has aimed for better technical governance standards, economic development, and social service delivery. Around two-thirds of EU development aid for ‘good governance’ has gone to governments and state institutions. It is doubtful that this is the optimal strategy for dealing with the specific challenges of digital repression. This requires a more political approach to human rights and democracy, which does not rely so heavily on such technocratic cooperation. While the EU has improved its policy tools in recent years, it cannot yet be concluded that it has yet made a complete transition.

Is digital repression a primary geopolitical interest? Tensions exist between the EU’s digital geopolitics and its commitments to advance democracy and human rights. It has shifted to prioritising digital sovereignty and boosting its relative power in technology against other powers. This is arguably beginning to side-line the rights dimension of digital strategies, and taking the EU back to a highly securitised approach to technological challenges, reminiscent of the early use of the cybersecurity concept. For all of the improvements in EU funding instruments and digital projects in third countries, it is not clear that, at the highest political level, all EU institutions and governments see the surge in digital authoritarianism itself as a geopolitical issue.

Lessons from Pegasus. The EU toolkit needs to be strengthened and made more precisely tailored to the spyware challenge. Significantly, upgraded measures are needed in respect of both vendors and governments using spyware for rights-infringing ends. Recommended measures, presented in detail in the next section, include tightening internal regulations among EU member states regarding export controls and the procurement of spyware from external countries, including non-Wassenaar countries; engaging in direct discussions with Israel regarding tightened export controls and more accountable licensing of spyware products and setting standards and guidelines for sanctions and conditionality in respect of spyware, among others. The EU has moved on some fronts in trying to fine-tune its toolbox to ‘catch up’ with the specificities of the spyware challenge, although beyond trade related issues its coverage of the wider geopolitical dimensions remains relatively limited.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1. Conclusions and recommendations in relation to the initial study

The proliferation of new and emerging technologies over the past two decades has significantly expanded states’ toolkits for repression and social control, deepening human rights problems. While they still have positive potential to enhance democratic values and human rights, these technologies are now also actively deployed and shaped by many repressive regimes to their own strategic advantage.

Globally and regionally, efforts have been made to tackle the challenge that digital technologies can pose to human rights, but much remains to be done. The EU must both enrich global legal and standard-setting efforts, and also improve its own core foreign policy instruments. The EU’s foreign policy toolbox has become more comprehensive in the last several years, as the EU has added a number of different strands to its efforts against digital authoritarianism. The challenge of digitally-led authoritarianism has continued to deepen, however, and the EU will need to look for ways to continue fine-tuning and adding to this toolbox. A core finding that runs through this report is that the EU has undertaken many valuable and well-designed policy initiatives in this field, but still has to decide whether tackling digital repression is a core geopolitical interest at the highest political level.

In order to take the EU’s fledgling efforts against digital repression further, a series of recommendations is offered below that encompass both the international human rights framework and the EU’s own, more specific, foreign policy framework. These two levels are equally important and need to dovetail with each other more effectively if the EU is to advance a fully comprehensive and multi-level approach to digital repression.

Putting more pressure on third countries

• In addition to all these ideas related to legal instruments, standard-setting, and stakeholder dialogue, the EU needs to include digital repression as a more central part of its high-level diplomacy and geopolitical strategies. Despite the rhetoric around digital repression and authoritarianism spreading globally, in practice, the EU places many other issues higher on its list of priorities with other governments. While seeking better global standard-setting, the EU cooperates on a range of security and commercial issues with some of the most digitally repressive regimes in the world, and has made moves to improve relations with such powers. For this to change, the EU must understand such digital trends as a core element of its geopolitical panorama, and not a minor human rights add-on to its core diplomacy.

• In order to make the many multilateral standard-setting forums and exercises more meaningful, the EU should link these to on-the-ground political developments. The EP should play a prominent role in pushing for the EU’s range of dialogues on human rights and positions in multilateral forums to address such developments, and not to focus solely on generic internet and digital standards abstracted from national political challenges. Rules, standards, and dialogues need to address concrete crisis situations where digital repression is mobilised at specific moments to deepen authoritarianism. In this, the EU needs to move beyond its much-improved capacities for early warning (including of threats to democracy and human rights) to early action.

• Sanctions are unlikely to be the leading instrument in EU human rights policies, but modest scope may exist to tighten the link between the Union’s restrictive measures and digital repression. The 2015 EP resolution mentioned in the previous chapter called for essential
elements clauses referring specifically to the need to respect ‘digital freedoms’, and for unhindered access to the internet, to be included in all new trade agreements. While the EU invokes such clauses relatively infrequently, this would still be a useful step to increase the importance of this issue on the EU’s external agenda. The new Global Human Rights Sanctions regime could also be widened by referring more explicitly and extensively to the multiple strands of digital repression covered in this study. The EU still needs to invest in the capacity and monitoring necessary to identify and unpack overt and more subtle forms of digital repression, and stipulate how they contribute to gross human rights violations of the type that might be liable to restrictive measures. This is a difficult task, as regimes’ digital tactics are nested within their wider range of power-maintenance strategies, but it might help to check the most draconian cases of digital repression. Even if sanctions need to be used sparingly, some regimes’ use of digital control is, at points, so severe that the EU should be willing to consider more concrete responses.

- The EU could and should use positive conditionality more systematically to leverage positive changes away from digital repression. Where third-country governments agree to work with the Union to reform restrictive laws and incorporate international standards, the EU should respond with additional aid, trade, and strategic benefits. This graded approach to political leverage would help deal with the problem of gradual autocratisation that the previous chapter outlines as one of the EU’s Achilles heels in recent years.

- Approaches to digital technology need to move away from security- and towards rights-based measures. The EU’s fast-growing array of cyber-security work has begun to incorporate a focus on digital rights, but a lot could (and still needs to) be done to fuse the security and human rights elements of the Union’s digital strategies. The same applies to Stratcom, the valuable work of which remains, as yet, somewhat disconnected from core EU human rights and democracy support. The EU would benefit from a formal liaison or contact point to link together the multiple cyber-security and human rights initiatives described above. EU pressure on cyber-security should align with pressure on human rights and democracy concerns.

Putting more pressure on the private sector

- The EU should increase the pressure it puts on private company operations in third countries, extending the ways it has begun to push them to adhere to more rigorous standards within the EU itself in recent years. This could take the form of a code or set of guidelines pertinent to companies’ stances on internet shutdowns and acute forms of digital repression outside of Europe. Where companies are found to be complicit in such digital repression, guilty of censorship themselves, or in breach of the UN Guiding Principles on Business and Human Rights, the EU might (as suggested in the 2015 EP resolution) subject them to certain forms of penalty, like exclusion from EU contracts – even if, generally, the EU (rightly) continues to prioritise efforts aimed at positive dialogue and cooperation.

- The EU needs to be also more attentive to the problem of ‘privatised censorship’ – that is, online platforms taking voluntary decisions that have negative effects on freedom of expression, as was recently the case when activists from the MENA region were blocked by Facebook and Twitter (see Chapter 3). As the EU is currently working on a legislative proposal to curb the arbitrariness of such practices of online platforms as part of the DSA-DMA package, it also needs to stress this problem in its external actions. Users in other parts of the world still lack protection against big tech’s decisions that undermine their fundamental rights. Given the European Commission’s experience in engaging in dialogue with dominant online platforms
in the area of content moderation\textsuperscript{453}, it should extend these efforts to support platforms’ user rights in other regions, leading the push for protection against unfair, non-transparent, and arbitrary removals.

**Increasing resources, funding, and capacity**

- The most impressive area of improvement in EU external initiatives is the Union’s range of funding for digital rights in third counties. This is important because it seeks to deal with digital repression through the positive approach of equipping local societies to defend their own human rights and explore the positive democratic potential of digital technology. Still, given the relatively modest amount of funding that has so far gone to such digital empowerment projects, the EU could and should significantly increase it. The EU could pick up a suggestion made in the EP’s 2015 resolution for a ‘human rights and technology fund’ to be created under the EIDHR (or now, its thematic successor). The EU has undertaken extremely valuable and creative work in protecting human rights defenders, including through digital tools. The challenge in building from this role will be for the Union to help create longer-term, systemic civic capacities to keep democratic spaces open, through a combination of joint online and offline techniques.

- The EP can play a valuable role here, using its cooperation with parliaments around the world to engage politicians with such civic initiatives as a means of amplifying their political impact. Given its key role in election observation, the EP would also be well placed to support a large-scale expansion of the EU’s fledgling and highly welcome efforts to build digital elements into its Election Observation Missions (EOMs) – this would be a natural area of partnership between the EP and the European External Action Service (EEAS). The EP could also push for increased levels of support to the European Endowment for Democracy (EED) and other foundations that are well equipped to take risks in pushing back against digital repression in the most difficult contexts.

- The EU should invest more resources in fostering wider coalitions of engagement. Any work in the field of human rights and new technologies, whether undertaken by human rights organisations or the EU, in an internal or external context, requires multi-stakeholder engagement. Apart from enhanced cooperation with the corporate sector, it is also essential to include other actors, particularly civil society and academia. Furthermore, such work requires adequate resources (human resources, in particular) to close the ‘knowledge gap’ between legal/human rights and technology experts.

- The EU should provide more resources to strengthen the rights-oriented monitoring of surveillance equipment exports, specifically. While the recast of the EU Dual-Use Regulation represents an important – if belated – step forward, tighter vigilance will be needed over the global spread of surveillance equipment beyond the tightly drawn terms of this regulation. The EP should support a dedicated initiative to monitor surveillance equipment exports from the EU, and – far from decreasing its focus on this issue now that the regulation is agreed – commit to working alongside civil society organisations to raise the profile of this issue.

**Extending the global reach of EU values through the regulation of new technologies**

- All actors in the EU, including the EP and the human rights community, should push strongly for a comprehensive, binding legal instrument to address the specific challenges posed by Al-
driven technologies. This should incorporate human rights safeguards into the entire life cycle of these technologies, including their design, deployment, and implementation, as well as into the full ‘datafication cycle’. The EU’s efforts to build its own legal framework for the development, design and application of AI technology should not be advanced in isolation from the existing instruments of different human rights organisations or their future improvement, such as the CoE’s potentially binding treaty on AI, which is currently under consideration. The European Commission should work towards ensuring consistency between EU and CoE legal frameworks on AI, as the latter could serve as a vehicle to promote the EU’s approach within non-EU CoE Member States, and potentially also beyond CoE countries, therefore helping to fulfil the Commission’s goal to ‘bring the Union’s approach to the global stage and build a consensus on human-centric AI’. The EP could contribute to global norms in particular by advancing dialogue with the US Congress to try to develop more common understandings, in particular on the norms governing AI and how these impact on human rights questions in both US and EU foreign policies.

- In light of its position as a global standard-setting actor, several other EU developments can help to reinforce multilateral efforts to strengthen the link between human rights and new technologies. This includes, in particular, GDPR, as well as planned or pending legislative initiatives, such as the DSA-DMA package and the EDAP, or possible future instrument(s) concerning mandatory due diligence for companies. Additionally, the ‘ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights’ could be used to develop more practical guidance on the application of the UN Guiding Principles to Digital Technologies, while the work of the EU Agency for Fundamental Right (FRA) in AI and discrimination and/or facial recognition could support human rights-based responses to tackling the rise of biometric surveillance in many parts of the world. These initiatives need to be incorporated fully into the EU’s ongoing dialogues with human rights organisations as a basis for tightening the human rights legal framework in this area, as well as in direct dialogue with partner countries across the globe. The EU could do more to promote its emerging standards for online platform regulation in third countries, where such rules and regulations remain much weaker.

In summary, there is scope for the EU to take actions at multiple levels at which it has begun to design responses to digital repression around the world. The EP is well placed to play a prominent role in assisting with and critically monitoring this area of policy development. One cross-cutting challenge is to ensure that the various strands of policy join together in a more coherent and high-profile commitment to tempering digital repression and expansive use of surveillance spyware. This trend is now of such a serious magnitude that it cannot be tackled through sporadic funding projects or multilateral standard-setting dialogues only; an EU policy that is fully commensurate with the scale of the technological challenge would place this issue at the highest political level of its overarching

---

454 Provided the future CoE instrument, like the 108+ or Budapest Conventions, is open for accession by States that are non-contracting parties of the CoE.


458 FRA (2018), #BigData: Discrimination in data-supported decision making.

foreign policy priorities. For all the progress the EU has made in recent years, this necessary steps are still to be taken.

5.2. Conclusions and recommendations in relation to Pegasus and equivalent surveillance spyware

Based on the update of the study, below we present recommendations on some parts of the EU toolkit that need to be strengthened and made more precisely tailored to the spyware challenge. Significantly, the following upgraded measures are needed in respect of both vendors and governments using spyware for rights-infringing ends:

- Most basically, the EU should give serious consideration to a moratorium on both the export and import of spyware. UN OHCHR and a large number of stakeholder groups and experts have called for a moratorium on the sale, transfer, and use of hacking tools until a human rights safeguards regime is in place.\(^{460}\) Such an action would be highly justified given the gravity of offenses and the range of documented human rights abuses linked to companies like NSO Group. While private firms claim they are adhering to human rights law and refusing to provide their tools to governments with repressive records, their records suggest otherwise. By hitting a pause on the private surveillance industry, this will bring incentives to establish robust transparency and accountability standards necessary to govern the sale, transfer, and use of hacking tools and mitigate abuses that have targeted journalists, activists, government critics, and human rights defenders.

- Separate from this and looking to the longer term, the EU should consider tightening export controls so that commercial surveillance vendors based in their own jurisdictions will meaningfully comply with core human rights standards, such as the UN Guiding Principles for Human Rights or the U.S. State Department’s “Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities.”\(^{461}\) It should add spyware-related specificity to the Recast Dual Use Regulation for this end. It might also use new due diligence framework to buttress such controls, although taking care not to over-stretch these due diligence rules and their focus on especially egregious rights abuses.

- The EU should also give as much attention to import as export controls, again in addition to the moratorium proposed above. EU security policy definitions need to specific how spyware links with certain types of regimes would sit uneasily with many of the EU’s own strategic interests. An instrument specific to import rules could enable the EU to tailor its approach to spyware around these quite specific and political questions. The EU should work towards tighter internal regulations among EU member states regarding the procurement of spyware from external countries, including non-Wassenaar countries. Currently, 12 EU members are deploying 15 Pegasus systems. In total there are 22 government organizations in EU countries using Pegasus (certain countries have reportedly purchased multiple spyware programs). The EU could send a powerful signal by making spyware infringements a part of its Defence of Democracy package due in 2023 – this is set to focus on outside threats to democratic

---

\(^{460}\) See for example: UN General Assembly, “The right to privacy in the digital age”, A/HRC/51/17

\(^{461}\) U.S. DEPARTMENT OF STATE, Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities; OHCHR (2011), Guiding Principles on Business and Human Rights Implementing the United Nations “Protect, Respect and Remedy” Framework
processes and so would resonate with the kinds of risks associated with spyware that this report has detailed.

- The EU should put more focus on rights concerns in its diplomatic discourse with Israel: the EU should engage in direct discussions with Israel regarding tightened export controls and more accountable licensing of spyware products given the centrality of Israeli companies in the global surveillance market and their association with a litany of harms. The EU of course has a range of other legitimate priorities in its engagement with Israel, but scope exists for deeper exchanges on spyware concerns.

- The EU should consider leveraging the Summit for Democracies to multilaterally tackle the spyware problem and to implement enforceable rules regarding the spread of dual use goods and technologies beyond the confines of the Wassenaar Arrangement. The 2021 Summit outcome document, for example, announced the establishment of a “multilateral initiative to develop rules of the road on the use and misuse of surveillance technology,” as well as a “multilateral export controls and human rights initiative” launched in partnership with Denmark, Norway, and Australia. But subsequent details have been scarce and there is uncertainty whether requisite political will exists to advance these proposals.

- The EU should use existing regulatory measures to hold the worst offenders in the commercial spyware industry legally accountable. For example, the EU could consider establishing a counterpart “entity list,” alongside the United States’ version, for companies engaged in egregious violations of human rights.

- EU governments should be more transparent regarding their own procurements and exports. As Ron Deibert writes, governments should treat surveillance vendors “with the same level of seriousness as some do the sale of advanced weaponry.” Governments could agree to only do business with surveillance firms that meet a certain threshold of due diligence around human rights compliance, based on measurable data and independent oversight: “such an ‘allow/deny’ list of vendors would not run the worst offenders out of business entirely, but it would marginalize them from some important marketplaces.” The EU should require robust due diligence and regular reporting by firms providing goods or services with surveillance capabilities to governments.

- The EU should consider enacting legislation that provides options for private litigation for victims of targeted surveillance against both governments and private companies. As Deibert writes, “governments hide behind foreign immunity provisions, and vendors may avoid responsibility for harm caused by their products when used by government clients.” Establishing laws that would create a right of action for victims to sue both commercial vendors and government clients in specific jurisdictions would increase liabilities and costs for companies, investors, and governments.

462 The White House (2021), Summit for Democracy Summary of Proceedings
463 Issues in Science and Technology (2022), Protecting Society From Surveillance Spyware
464 Issues in Science and Technology (2022), Protecting Society From Surveillance Spyware
465 Access Now (2021), Victory! U.S. blocklists NSO Group and Candiru
466 Issues in Science and Technology (2022), Protecting Society From Surveillance Spyware
The EU should encourage technology platforms, such as WhatsApp or iOS, whose infrastructure is routinely exploited by spyware firms, to set up a central litigation fund to facilitate users filing lawsuits against companies for violations of their terms of service and for other damages.

The EU should begin to address the wider geopolitics of spyware beyond export-import issues and the private sector. The EU has a huge number of core foreign policy documents, covering general geopolitical strategy, defence, human rights, trade and the like: as and when it moves gradually to update these, it could incorporate into the updated versions more specific references to spyware and its interaction with geopolitics – along the lines suggested in this report. Of course, such formal references might not in themselves have a dramatic impact on the challenges, but they would give the EU a stronger platform from which to make spyware issues a core part of its diplomatic processes. This would be an advance given that policymakers lament that such formal codified reference points are currently weak. In a recent EP-commissioned study, it is argued that tighter definitions of national security are required from member states (who have competence for security issues) to circumscribe what is a legitimate security use of spyware; if this is especially relevant to security actions within member states, it is an injunction that could usefully be followed for member states’ external security strategies too.

As part of this, and more specifically, the EU could draw up standards and guidelines for sanctions and conditionality in respect of spyware so that some kind of template exists for when third country governments are found to be using intrusive means against EU citizens or governments or their own civil societies. Sanctions are unlikely to be feasible or desirable method of responding to most spyware issues, but the EU might usefully draw red lines beyond which it deems repression to be so severe that some kind of response is warranted.

The EU could, for example, suspend security and CT cooperation with regimes using Pegasus on opposition figures and human rights defenders. At the least, the EU should ensure its own aid – security aid and research funds like Horizon – and not directly contributing to regimes’ use of intrusive spyware. MEPs have already called for EU to look at Horizon funding to Israel. The use of instruments like the EU Guidelines on Human Rights Defenders could be made more systematic and high-level in raising concerns where third-country governments are using spyware against the very individuals and organisations that the EU is supporting for human rights work.

The EU could design a dedicated funding initiative or call for proposals related to the human rights dimensions of spyware and make this available for victims of spyware seeking to continue work as democracy and human rights activists. The various strands of useful EU funding related to digital security and pushing back against digital authoritarianism could be upgraded and their spyware elements coalesced into an initiative with greater political impact.

467 G. Sartor and A. Loreggia, The impact of Pegasus on fundamental rights and democratic processes, Study requested by the PEGA Committee
REFERENCES

Primary Sources


- Council of Europe Ad Hoc Committee on Artificial Intelligence (CoE CAHAI), ‘Feasibility study’, 2020. Available at: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da


- Council of Europe Commissioner for Human Rights, ‘Positions on Counter-Terrorism and Human Rights Protection’, 5 June 2015. Available at: https://rm.coe.int/16806db6b2


Council of Europe Committee of Ministers, ‘Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes’, 2019. Available at: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

Council of Europe Committee of Ministers, ‘Recommendation CM/Rec (2019)2 on the protection of health-related data’, 2019. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e


Council of Europe Committee of Ministers, ‘Recommendation on preventing and combating sexism’, CM/Rec(2019)1, 2019. Available at: https://rm.coe.int/168093b26a


Council of Europe Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing (CoE T-PD), ‘Guidelines on the protection of individuals wih regard to the processing of personal data in a world of big data’, 2017. Available at: https://rm.coe.int/16806ebe7a

Council of Europe Cybercrime Convention Committee (T-CY), ‘Mapping study on cyberviolence’, 2018. Available at: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

Council of Europe European Committee on Crime Problems (CPDC), ‘Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law’, 2020. Available at: https://rm.coe.int/cdpc-2020-3-feasibility-study-of-a-future-instrument-on-ai-and-crimina/16809f9b60
- Council of Europe, ‘Chart of signatures and ratifications of the European Convention of Human Rights (‘ECHR’). Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures
- Council of Europe, ‘Chart of signatures and ratifications of the European Social Charter (‘ESC’). Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/163/signatures
- Council of Europe, ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data’, ETS No. 108., 1981. Available at: https://rm.coe.int/1680078b37
- Council of Europe, ‘Convention on preventing and combating violence against women and domestic violence’, CETSNo.210, 2011. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000168008482e
- Council of Europe, European Committee on Crime Problems (CDPC), ‘Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law’, 4 September 2020. Available at: https://rm.coe.int/cdpc-2020-3-feasibility-study-of-a-future-instrument-on-ai-and-crimina/16809f9b60


• European Commission, ‘The List of all EU sanctions’. Available at: www.sanctionsmap.eu/#/main


• European Court of Auditors, ‘Challenges to effective EU cybersecurity policy’, Briefing paper, 2019. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
European Court of Human Rights, ‘Bulgakov v. Russia’, 2015/19. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-203181%22]}

European Court of Human Rights, ‘Engels v. Russia’, 61919/16, 23 June 2020. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-203180%22]}


European Court of Human Rights, ‘OOO Flavus and Others v. Russia’, 12468/15, 23 June 2020. Available at: https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-203178%22]}


• OHCHR Accountability and Remedy Project. Available at: www.ohchr.org/EN/Issues/Business/Pages/OHCHRaccountabilityandremedyproject.aspx


Pegasus and the EU’s external relations

- OSCE Representative on Freedom of the media, ‘Impact of Artificial Intelligence’. Available at: https://www.osce.org/fom/ai-free-speech
- OSCE, ‘Communiqué by the OSCE RFoM on Media Pluralism, Safety of Female Journalists and Safeguarding Marginalized Voices Online’, 2019. Available at: www.osce.org/representative-on-freedom-of-media/411917
- OSCE, ‘Joint declarations. Available at https://www.osce.org/fom/66176
- OSCE, ‘Recommendations on Countering Online Abuse of Female Journalists’, 21 October 2015. Available at: www.osce.org/fom/193556
- The Wassenaar Arrangement Secretariat. Available at: www.wassenaar.org

• UN Data Revolution, ‘A World that Counts Mobilising the Data Revolution for Sustainable Development’, 2014. Available at: www.undaterevolution.org/report/


• UN General Assembly, ‘Resolution on the safety of journalists and the issue of impunity’, A/RES/72/175, 2017. Available at: https://digitallibrary.un.org/record/1467885

• UN General Assembly, ‘Right to Privacy in the Digital Age’, Resolution A/RES/73/179, 2018. Available at: https://digitallibrary.un.org/record/1661346


• UN General Assembly, Resolution A/RES/75/176, 2020. Available at: https://undocs.org/A/RES/75/176


• UN Human Right Council, ‘Resolution 32/10’, 15 July 2016. Available at: https://undocs.org/A/HRC/RES/32/10


• UN Human Right Council, ‘Resolution 44/15’, 23 July 2020. Available at: https://undocs.org/A/HRC/RES/44/15


• UN Human Rights Committee, ‘General comment no. 37 on the right of peaceful assembly’, 2020. Available at: https://digitallibrary.un.org/record/3884725


• UN Human Rights Council, ‘New and emerging digital technologies and human rights’. Available at: https://www.ohchr.org/EN/HRBodies/HRC/AdvisoryCommittee/Pages/DigitalTechnologiesandHR.aspx


• UN Human Rights Council, ‘Resolution 26/22’, 23 July 2020. Available at: https://undocs.org/A/HRC/RES/44/15


• UN Human Rights Council, ‘Resolution A/HRC/44/L.11’, 2020


• UN Secretary General, ‘Strategy on new technologies’, 2018. Available at: www.un.org/en/newtechnologies


• UN Special Rapporteur on extreme poverty and human rights, ‘Report A/74/493’, 11 October 2019. Available at: https://undocs.org/A/74/493


• UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and Access to Information, ‘Joint Declaration on Freedom of Expression and Responses to Conflict Situations’, 4 May 2015. Available at: https://www.osce.org/fom/154846


• UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ‘Report no. A/70/361’, 2015. Available at: https://digitallibrary.un.org/record/805706

• UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ‘Report no. A/HRC/23/40’, 2013. Available at:
Pegasus and the EU's external relations


- UN Special Rapporteur on the right to privacy, ‘Report no. A/74/277’, 2019. Available at: https://undocs.org/A/74/277

- UN Special Rapporteur on the right to privacy, ‘Report no. A/75/147’, 2020. Available at: https://undocs.org/A/75/147


- UN, ‘Chart of signatures and ratifications of the 4. International Covenant on Civil and Political Rights(ICCPR)’ Available at: https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND
• UN, ‘Chart of signatures and ratifications of the International Covenant on Economic, Social and Cultural Rights (‘ICESCR’). Available at: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-3&chapter=4&clang=_en


• United Nations Hub for Human Rights and Digital Technology. Available at: https://www.digitalhub.ohchr.org/


• U.S. Security and Exchange Commission, Registration No. 333-256177, Cellebrite Ltd., 29 June 2021. Available at: https://www.sec.gov/Archives/edgar/data/1854587/000121390021034768/ff42021a1_cellebrite_di.htm#T23
Secondary Sources – books and articles


• Collins, K., ‘Hacking Team’s oppressive regimes customer list revealed in hack’, Wired, 7 June 2015. Available at: https://www.wired.co.uk/article/hacking-team-spyware-company-hacked


• Degani, C., ‘An Elite Israeli Intelligence Unit’s Soldiers Are Sworn to Secrecy – but Tell All on LinkedIn’, Haaretz, 18 November 2021. Available at: https://www.haaretz.com/israel-news/tech-news/2021-11-18/ty-article/.premium/an-israeli-intell-units-soldiers-are-sworn-to-secrecy-but-tell-all-on-linkedln/0000017f-e0e5-d568-ad7f-f3ef63350000


Pegasus and the EU's external relations


- Gebrekidan, S., ‘For autocrats and others, coronavirus is a chance to grab even more power’, New York Times, 30 March 2020. Available at: https://www.nytimes.com/2020/03/30/world/europe/coronavirus-governments-power.html


• Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J. and Deibert, R., ‘We Chat, They Watch: How International Users Unwittingly Build Up WeChat’s Chinese Censorship Apparatus’, Citizen Lab, University of Toronto, 7 May 2020. Available at: https://citizenlab.ca/2020/05/we-chat-they-watch

Kostka, G., ‘China’s social credit systems and public opinion: Explaining high levels of approval’, New Media & Society, 27(7), 2019. Available at: https://journals.sagepub.com/doi/full/10.1177/1461444819826402


MacKinnon, R., ‘Chinese tech giants can change: But the state is still their number one stakeholder’, 2021. Available at: https://rankingdigitalrights.org/index2020/spotlights/china-tech-giants


• Marczak, B., Scott-Railton, J., Senft, A., Poetranto, I., and McKune, S. ’Pay No Attention to the Server Behind the Proxy: Mapping FinFisher’s Continuing Proliferation’ Citizen Lab, University of Toronto, 15 October 2015. Available at: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/  


• Meaker, M., ‘Spyware Scandals Are Ripping Through Europe’ Wired, 15 August 2022. Available at: https://www.wired.com/story/europe-spyware-scandals-greece/  


• Roussi, A., ‘EU spyware inquiry fails to put Spain on list of fact-finding trips’, Politico, 7 July 2022. Available at: https://www.politico.eu/article/pedro-sanchez-spain-spyware-inquirys-visit-falls-flat-for-fear-of-embarrassment/


• Santa Clara Principles on Transparency and Accountability in Content Moderation, 2018. Available at: https://santaclaraprinciples.org/


Pegasus and the EU’s external relations


- von Ow-Freytag, B., ‘Filling the void: why the EU must step up support to Russian civil society’, Martens Centre for European Studies, 2018. Available at: https://journals.sagepub.com/doi/full/10.1177/1781685818813294


Joint/ Group Publications

• Access Now, ‘#KeepItOn: Open letter appealing to the Deputy Director-General to urge the governments of Bangladesh, India, Myanmar, and Pakistan to end the ongoing internet shutdown amid COVID-19 pandemic’, 26 May 2020. Available at: www.accessnow.org/civil-society-to-wholets-end-government-ordered-internet-shutdowns


• Access Now, ‘Cutting internet access when people need it the most: stories from Uganda’, 9 February 2021. Available at: https://www.accessnow.org/internet-shutdown-stories-from-uganda/


• Access Now, ‘Rights groups to Facebook on Tunisia’s “disappeared” accounts: we’re still waiting for answers’, 23 June 2020. Available at: https://www.accessnow.org/rights-groups-to-facebook-on-tunisias-disappeared-accounts-were-still-waiting-for-answers

Pegasus and the EU’s external relations


- CISA, ‘Understanding Denial-of-Service Attacks’, November 2019

- Citizen Lab, University of Toronto, ‘Communities @ Risk: Targeted Digital Threats Against Civil Society’, 11 November 2014. Available at: https://targetedthreats.net/media/1-ExecutiveSummary.pdf

• Crowdstrike, ‘Advanced Persistent Threat (APT)’, 15 June 2022. Available at: https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

• Democracy Support and Election Coordination Group. Available at: https://www.europol.europa.eu/globaldemocracysupport/en/home/democracy-group


• Digital Freedom Fund. Available at: https://digitalfreedomfund.org/


• Financial Times, ‘EU pressured to give results of leak probe on China disinformation’, 21 June 2020. Available at: https://www.ft.com/content/5a323cec-82a6-4e64-9bbb-27e8de7b9929


• Freedom Online Coalition. Available at: www.freedomonlinecoalition.com


• ICFJ, ‘ICFJ-UNESCO Global Study: Online Violence Against Women Journalists’, 2020

• Internet Governance Forum. Available at: www.intgovforum.org


• Lighthouse Reports, ‘Revealing Europe’s NSO’, 28 August 2022. Available at: https://www.lighthousereports.nl/investigation/revealing-europes-nso/

• Mendeley Data, ‘Commercial Spyware Global Inventory’, 12 December 2020. Available at: https://data.mendeley.com/datasets/csvhpkt8tm/1


Pegasus and the EU’s external relations


List of consulted stakeholders

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Interviewee</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>24.11.2020</td>
<td>Interview with key informant, under full anonymity</td>
</tr>
<tr>
<td>2.</td>
<td>26.11.2020</td>
<td>Interview with key informant, under full anonymity</td>
</tr>
<tr>
<td>3.</td>
<td>27.11.2020</td>
<td>Interview with four representatives of EU institution</td>
</tr>
<tr>
<td>4.</td>
<td>02.12.2020</td>
<td>Interview with a representative of EU institution</td>
</tr>
<tr>
<td>5.</td>
<td>02.12.2020</td>
<td>Interview with two representatives of the EEAS</td>
</tr>
<tr>
<td>6.</td>
<td>03.12.2020</td>
<td>Interview with three key informants, under full anonymity</td>
</tr>
<tr>
<td>7.</td>
<td>09.12.2020</td>
<td>Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales</td>
</tr>
<tr>
<td>8.</td>
<td>09.12.2020</td>
<td>Interview with a representative of EU institution</td>
</tr>
<tr>
<td>9.</td>
<td>15.12.2020</td>
<td>Interview with a representative of EU institution</td>
</tr>
<tr>
<td>10.</td>
<td>17.12.2020</td>
<td>Interview with Jonathan McCully, Legal Adviser, Digital Freedom Fund</td>
</tr>
<tr>
<td>11.</td>
<td>17.12.2020</td>
<td>Interview with a representative of EU institution</td>
</tr>
<tr>
<td>12.</td>
<td>22.12.2020</td>
<td>Interview with a representative of the European Endowment for Democracy</td>
</tr>
<tr>
<td>13.</td>
<td>06.01.2021</td>
<td>Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now</td>
</tr>
<tr>
<td>14.</td>
<td>08.01.2021</td>
<td>Interview with Diego Naranjo, Head of policy, European Digital Rights</td>
</tr>
<tr>
<td>15.</td>
<td>08.01.2021</td>
<td>Interview with Patrick Penninckx, Head of the Information Society Department of the Council of Europe</td>
</tr>
<tr>
<td>No.</td>
<td>Date</td>
<td>Activity</td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>16</td>
<td>14.01.2021</td>
<td>Interview with a representative of an international institution</td>
</tr>
<tr>
<td>17</td>
<td>20.01.2021</td>
<td>Interview with private sector representative</td>
</tr>
<tr>
<td>18</td>
<td>29.01.2021</td>
<td>Online written consultation with a representative of EU institution</td>
</tr>
<tr>
<td>19</td>
<td>12.03.2021</td>
<td>Interview with a representative of EU institution</td>
</tr>
<tr>
<td>20</td>
<td>31.10.2022</td>
<td>Interview with a representative of EU institution</td>
</tr>
<tr>
<td>21</td>
<td>12.2022</td>
<td>Interview with a representative of EU institution</td>
</tr>
</tbody>
</table>
ANNEXES

Interview topic guide – EU institutions


INTERVIEW TOPIC GUIDE

(AND REPORT TEMPLATE)

EU institutions version

Instructions for the interviewer:

Before the interview:

• Familiarise yourself with the legal mandate of the interviewee’s institution and the responsibilities of the interviewee’s specific unit/department vis-à-vis EU foreign policy.

Immediately before beginning the interview:

• Confirm whether the interviewee agrees to the interview.

• Determine whether and how the interviewee would like to be quoted in the final paper:
  o ☐ Full citation with name and organisational affiliation;
  o ☐ Citation of only my position and organisational affiliation;
  o ☐ Citation of only my organisational affiliation; or
  o ☐ Citation only in terms of sector (i.e. representative of EU institution etc.).

• Ask for permission for recording and explain that recording is voluntary and only for internal purposes to prepare write-ups from interviews.

• Once recording is switched on, confirm that the consent for recording was obtained.

• Explain to the interviewee that the study relates to the problem of using digital technologies for repression and social control. Clarify that its main purposes are to: (1) provide an overview of the international HR framework which is relevant to this phenomenon and (2) describe and assess relevant EU foreign policy framework and toolbox with the view to its effectiveness and completeness, as well as available expertise and resources. Underline that in the interview, we will concentrate on obtaining better understanding of the options that the EU has in its foreign policy toolbox to address such use of digital technologies and learning how effective the toolbox is in practice.
It should also be made very clear that the study is only about human rights impacts in third countries. This is important because with the discussion about foreign disinformation (which is partly based on the use of digital technologies), foreign policy tools are also used to address human rights impacts within the EU and its MS.

Part 1. Use of digital technologies for repression and social control

1. Have you noted, as part of your work, instances when digital technologies were used by the authorities in third countries for repression and social control?

2. (if YES to Q1, and based on the interviewee’s professional experience) What are some of the new and emerging digital technologies that have the most significant impact on human rights? How are these technologies used for repression and social control?

3. (if YES to Q1, and based on the interviewee’s professional experience) From the EU perspective, what are the key human rights challenges arising from the use of digital technologies?

Part 2. Interviewee’s involvement in EU foreign policy

4. Could you briefly explain your role within your institution? (What is your area of responsibility in relation to EU foreign policy?) (if not addressed earlier, or to confirm understanding – then rephrase appropriately)

5. What EU policy instruments do you work with? (alternative: What is your mandate vis-à-vis specific instruments?) (if not addressed earlier, or to confirm understanding – then rephrase appropriately)

6. Could you briefly explain how you work with those instruments? What does it look like in practice/on the ground? (if not addressed earlier, or to confirm understanding – then rephrase appropriately)

Part 3. EU instruments responsive to the abuse of digital technologies

7. Which, if any, EU foreign policy tools that you have experience with (at the disposal of your institution) allow the EU (in one way or another) to address/respond to the use of digital technologies for repression and social control?

8. How can these instruments be used to tackle the use of digital technologies for repression and social control? (if not addressed earlier, or to confirm understanding – then rephrase appropriately)

9. Do you recall any instances when specific foreign policy instruments were applied to tackle the use of digital technologies for repression and social control? Could you describe some examples?

Part 4. Effectiveness of EU foreign policy instruments in tackling the use of digital technologies for repression and social control

10. (If YES to Q9) To what extent does the application of the EU foreign policy instruments that you have at your disposal contribute to limiting the use of digital technologies for repression and social control or to limiting the impact of such use on targeted people/communities?

a. In situation that you recalled earlier (under Q9), how did the applied measures work in practice? Was there any change in response to their application?
b. From the perspective of tackling the use of digital technologies for repression and social control, what are the strengths and weaknesses of specific tools/instruments that you work with?

11. Are you able to determine which measures (or combinations of measures) have more impact on the practices in third countries? (i.e., better help to limit/curb the use of digital technologies for repression and social control)

12. In your view, what factors influence (or can influence) the effectiveness of applied EU foreign policy tools?

13. What conditions help to increase the effectiveness of EU foreign policy tools?

**Part 5. Comprehensiveness of EU foreign policy instruments in tackling the use of digital technologies for repression and social control**

14. Does the EU foreign policy toolbox allow the EU to properly tackle all instances when digital technologies are used for repression and social control?
   a. *(If YES to Q13)* Would you then say that the instruments are used to their full potential at the moment? If NOT, why? What should change in the practical application of those instruments?
   b. *(If NO to Q13)* Why not? Are there any instruments/solutions missing? What are those missing instruments/solutions? Can you recall any tools that were put forward in the past, but did not materialise/did not get adopted? Why?

**Part 5. Available resources and expertise**

15. *(in the context of dynamically developing digital technologies)* What is your assessment of the resources and expertise within your institution to properly respond – using the available EU foreign policy tools – to the use of digital technologies for repression and social control?

**Part 6. International/regional HR framework**

16. In your view, can the existing international or regional human rights framework address the problem of digital technologies being used as means of repression and social control?
   a. Is the framework sufficient? If NO, what is missing?
   b. What can the EU do to improve this framework?

17. Is there anything you would like to add before we finalise the interview?
Interview topic guide – CSOs and other respondents


INTERVIEW TOPIC GUIDE

(AND REPORT TEMPLATE)

CSOs & other respondents version

Instructions for the interviewer:

Immediately before beginning the interview:

• Confirm whether the interviewee agrees to the interview.

• Determine whether and how the interviewee would like to be quoted in the final paper:
  o ☐ Full citation with name and organisational affiliation;
  o ☐ Citation of only my position and organisational affiliation;
  o ☐ Citation of only my organisational affiliation; or
  o ☐ Citation only in terms of sector (i.e. representative of EU institution etc.).

• Ask for permission for recording and explain that recording is voluntary and only for internal purposes to prepare write-ups from interviews.

• Once recording is switched on, confirm that the consent for recording was obtained.

• Explain to the interviewee that the study relates to the problem of using digital technologies for repression and social control. Clarify that its main purposes are to: (1) provide an overview of the international HR framework which is relevant to this phenomenon and (2) describe and assess relevant EU foreign policy framework and toolbox with the view to its effectiveness and completeness, as well as available expertise and resources. Underline that in the interview, we will concentrate on obtaining better understanding of the options that the EU has in its foreign policy toolbox to address such use of digital technologies and learning how effective the toolbox is in practice.

Trends in the use of new technologies for repression and social control

1. What are new and emerging digital technologies that have the most significant impact on human rights (in the context of repressions or/and social control) in the recent years, used globally or/and in the region where you work? What are the key human rights challenges arising from the use of those technologies? Is there anything in particular that makes today’s digital technologies different from earlier periods?

2. Could you give at least one example of the application of such technologies (in particular in the region where you work)?
3. Do you observe any other trends/phenomena in actions taken by state actors in relation to new technologies that have negative implications for human rights globally/in the region where you work (such as export/import of new technologies that are then used for widespread surveillance, internet shutdowns, extending surveillance powers of state agencies by legislation etc.)? Please provide concrete examples to the extent possible.

4. What (which countries) are the global/regional “leaders” in using new technologies (and/or setting/applying the above-mentioned trends) in a way that may challenge human rights? Please justify your choice.

5. Are there any particular groups most vulnerable to the negative impact of those actions? (racial, gender, religious, social, political etc.)

6. What is the role of private actors in this context? Which categories of private actors are particularly critical? (e.g. internet platforms, companies producing surveillance technologies) Could you give examples?

7. What is the impact of the COVID-19 pandemic on the use of new technologies that may have negative implications for human rights (in particular in the region where you work)?

8. Have there been any other particular events (protests, elections etc.) in the recent years which triggered an increased use of new technologies with negative implications for human rights in the region where you work?

9. Could you point us towards the recent key publications/accomplishments/other developments of your organization on the issue of new digital technologies and human rights?

International HR legal framework

10. What is your general assessment of the current international HR legal framework related to the use of new digital technologies? Is it adequate and effective in addressing human rights challenges posed by those technologies?

11. Can you observe any particular trends in how HR systems have been responding in the recent years (or may respond in the near future) to the challenges related to the use of new digital technologies for repression and social control?

12. What are the major problems or gaps in the current HR legal framework (such as important technologies/areas that have been overlooked or that need to be further addressed or standards that are inadequate or insufficient in the context of actual challenges)?

13. What are the most important issues that should be considered on the current agendas of the international HR bodies? What types of reforms are needed to improve the existing HR legal framework?

14. Do you observe any particular clashes/discrepancies between different HR systems (universal vs. regional, different regional ones) regarding the use of new technologies?

15. Can you identify any examples of particularly important developments/good practices undertaken by international HR bodies in the context of risks arising from new digital technologies?
16. What is your assessment of the current HR legal framework as far as human rights obligations of private actors in the technological field are concerned? Are they comprehensive, sufficient and effective?

17. What is your assessment of the responses of the different international HR systems to the COVID-19 crisis? Does the pandemic affect the ways in which international HR standards should apply to tech companies?

18. Is there anything else that you would like to add?
This study - commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs at the request of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA) — analyses the proliferation of new and emerging technologies used for repression and social control. While these technologies still have the potential to positively enhance democratic values and human rights, repressive regimes actively deploy these tools for their own strategic advantage. In particular, the proliferation of commercial spyware, such as Pegasus software, is a big concern. The EU should place a much higher priority in countering government use of these tools.