# EXECUTIVE SUMMARY

## Study for the PEGA Committee

European Parliament

# Pegasus and the EU's external relations [1]


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.


## Assessment of the EU policy toolbox

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, 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 leant themselves easily to

[1] Full study in English: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/741475/IPOL_STU(2023)741475_EN.pdf


Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 741.475 - June 2023

SR 1277110EN

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 on 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

External Authors: Prof. Steven FELDSTEIN, Senior Fellow, Carnegie Europe, Brussels
Prof. Richard YOUNGS, Senior Fellow, Carnegie Europe, Brussels & Professor of International Relations, University of Warwick, UK

Research Administrator responsible: Mariusz MACIEJEWSKI, Ottavio MARZOCCHI Editorial assistant: Ivona KLECAN

Contact: poldep-citizens@europarl.europa.eu

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

PE 741.475
IP/C/PEGA/IC/2022-082

Print ISBN 978-92-848-0783-3 | doi: 10.2861/992562 | QA-09-23-266-EN-C
PDF ISBN 978-92-848-0780-2 | doi: 10.2861/667512 | QA-09-23-266-EN-N