Taking Stock “Commercial Spywares And Beyond” : Multistakeholder Convening at the 2023 Paris Peace Forumfocusing on tackling the risk of the irresponsible use and proliferation of commercial cyber tools, including commercial spyware

**The misuse and proliferation of commercial cyber tools first became a major policy issue a decade ago. European governments and the U.S. government subsequently paid closer attention to the use and exports of such technologies.** Partly fueled by national security and counterintelligence concerns complementing those raised by human rights organizations, governments supported the addition of two new multilateral export controls dedicated to commercial cyber tools through the Wassenaar Arrangement in 2013.[[1]](#endnote-2) The strategic goal is to shape the marketplace in support of the responsible use consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties and in line with the UN Guiding Principles for Business and Human Rights..

**Over the past decade, the misuse and proliferation of commercial cyber tools has been a growing concern** of governments. For example,

* The U.S. Office of the Director of National Intelligence warned as early as 2013 that “a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems.”[[2]](#endnote-3) In 2020, President Trump highlighted “the proliferation of more effective and commercially available cyber and surveillance technologies” as a concern in the US National Counterintelligence Strategy.[[3]](#endnote-4)
* In France, the 2018 Cyber Defence Strategic Review points to the need to regulate “cyber offensive activities” specifically highlighting the role of export controls.[[4]](#endnote-5) France’s 2022 National Strategy Review further highlights that “sophisticated off-the-shelf, cyber-espionage weapons and tools are gradually being developed by private companies. This cyber-arms race increases the risk of escalation, the stages of which are not equally understood.“ The document further notes that: “France must put forward proposals to control the trade in cyber weapons and fight against their proliferation, including through better use of export control schemes for goods and technologies”.[[5]](#endnote-6)
* In the United Kingdom, the 2022 National Cyber Strategy references “commercial spyware used to target activists, journalists, and politicians” among the cyber threats the country faces warning that “threats in cyberspace will continue to evolve and diversify as high-end cyber capabilities become commoditized and proliferate to a wider range of states and criminal groups.” With the Strategy, the government commits to “counter the proliferation of high-end cyber capabilities to states and organized crime groups via commercial and criminal marketplaces.”[[6]](#endnote-7) Deputy Prime Minister Dowden specifically pointed to “more and more adversaries [being] able to buy and sell sophisticated cyber tools and spyware like Pegasus.”[[7]](#endnote-8) A 2023 report by the UK National Cyber Security Centre focusing on the cyber threat evolution over the next five years, warns that “the irresponsible use of spyware against individuals is almost certainly happening at scale, with thousands of people targeted every year. We should expect to see high-profile exposures of victims who have been targeted through unethical and illegal use of sophisticated and cost-effective cyber tools or hackers for hire continue over the next five years.”[[8]](#endnote-9)

Over the same period, civil society organizations have continued to produce in-depth research shedding light on the continued misuse of technology, leading to increased frontpage covered in major international news outlets, such as The New York Times, about the growing industry.[[9]](#endnote-10) This research documented how the misuse of commercial cyber tools, namely commercial spyware, ranges from targeting journalists to European opposition leaders to other high-profile individuals.[[10]](#endnote-11) While European governments transposed the new Wassenaar export controls into their national export control regimes within a few years, the U.S. government did not finalize them domestically until 2021.[[11]](#endnote-12) One main reason was that the cybersecurity industry and researchers cautioned that the controls’ provisions focusing on the development of cyber tools could unintentionally undermine legitimate cybersecurity efforts.[[12]](#endnote-13)

**In 2021, the U.S. government significantly stepped up its activity to counter the misuse and proliferation of cyber tools, namely spyware, going beyond the actions initially taken**. The U.S. has taken unprecedented steps expanding the instruments of statecraft leveraged in this area combining the use of export controls, licensing policy, restrictions for US government employees, diplomacy, and new executive and legislative actions.[[13]](#endnote-14) In addition, in May 2023, the French President and the British Prime Minister agreed to “pursue their cooperation on cyber issues and give a new impetus to the UK-France Cyber Dialogue by pursuing a joint initiative to take forward international action on tackling the threat from commercial cyber proliferation, including commercial spyware.”[[14]](#endnote-15) Two weeks later, eleven countries issued a *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware* highlighting the unique momentum and growing international will to take action.[[15]](#endnote-16) Recognizing the Paris Call for Trust and Security in Cyberspace’s “non-proliferation” principle, it is similar but distinct to other international efforts which are complementary to each other.

**Shaping the international market of commercial cyber tools, including spyware, to address counterintelligence and national security concerns as well as the continuing misuse and human rights violations remains urgent and important.** It requires a continued strategic focus and dedicated action. One promising approach to make significant progress in this area in the coming months is to think of the issue set as a Ven diagram. Cyber tools encompass a broader range of technologies from network surveillance systems to intrusion software. Spyware is a particularly prominent subset of cyber tools because of its use targeting high-profile individuals and its impact, which includes a convergence of national security, cybersecurity, counterintelligence, and human rights concerns and relevant stakeholder communities.

**The Paris Peace Forum offers an opportunity to take stock of the ongoing efforts over the past decade and to**

1. **evaluate progress since the issuance of the Joint Statement;**
2. **expand and diversify the number of countries committing to its objectives; and**
3. **provides an opportunity to set priorities and develop action plans for the coming year.**

This would ideally not only focus on the governments’ ongoing efforts but also industry’s commitments outlined in the Cyber Tech Accord principles focusing on cyber mercenaries[[16]](#endnote-20) as well as civil society’s research and advocacy.[[17]](#endnote-21)

**Carnegie proposes to co-host a half-day event in the afternoon of November 9 with the French government and the Paris Peace Forum convening a multistakeholder group of key actors from governments, industry, and civil society in this area.** The in person event will be by invitation only.

PROPOSED AGENDA FOR NOVEMBER 9

[1200-1330: Potential Pre-Event Working Lunch limited to Governments.]

1330-1415: Welcome + Scenesetter + Introductions

1415-1530: Tackling the Proliferation of Commercial Spyware

* + Instruments of statecraft: inspiring examples of steps taken with the Joint Statement
  + How can industry and civil society help implement these instruments?
  + Call for commitments: how to extend the Joint Statement to new signatory countries?

1530-1600: Coffee Break

1600-1730: Going Beyond Spyware to Curb the Market of Cyber Offensive Capabilities

* + What are we talking about? Defining commercially-available cyber offensive capabilities.
  + How to build on the early lessons learned from commercial spywares?
  + Call for contributions: how to generate global response to the phenomenon?

1730: Reception

PROPOSED PARTICIPANTS FOR NOVEMBER 9 EVENT

* Governments (MFAs + representatives from other relevant ministries)
  + Core group: France, UK, US
  + Additional 8 countries that signed onto the Joint Statement in March 2023
  + Additional countries selected by core group:
    - Europe: Estonia, Germany, The Netherlands, Cyprus, Greece
    - Asia: Japan, ROK, Singapore
    - Africa: Ghana, South Africa
    - Latin America: Brazil
* Civil Society
  + Carnegie
  + Access Now
  + Amnesty
  + Citizen Lab
  + Committee to Protect Journalists
  + Cyber Peace Institute
  + Freedom House
  + Reporters without Borders
  + Chatham House
  + GEODE
  + Additional proposals from the [March 27 Civil Society Joint Statement](https://media.business-humanrights.org/media/documents/JointStatement_Summit_for_Democracy_2023_FINAL.pdf)
* Industry
  + Microsoft
  + Google
  + Meta
  + Apple
  + Cisco
  + Trend Micro
  + ESET
  + Avast
  + Sekoia.io

PROPOSED PARTICIPANTS FOR HIGH-LEVEL SEGMENT OF PARIS PEACE FORUM (November 10/11)

* Governments
  + Same as above + plus additional group of countries, e.g., ASEAN
* Civil Society
  + Same as above + others
* Industry
  + Same as above + others

REFERENCES

1. https://www.newamerica.org/oti/blog/a-guide-to-the-wassenaar-arrangement/ [↑](#endnote-ref-2)
2. https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf [↑](#endnote-ref-3)
3. https://www.dni.gov/files/NCSC/documents/features/20200205-National\_CI\_Strategy\_2020\_2022.pdf [↑](#endnote-ref-4)
4. https://www.sgdsn.gouv.fr/publications/revue-strategique-de-cyberdefense [↑](#endnote-ref-5)
5. https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022 [↑](#endnote-ref-6)
6. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/1049825/government-cyber-security-strategy.pdf [↑](#endnote-ref-7)
7. https://www.gov.uk/government/speeches/cyberuk-speech [↑](#endnote-ref-8)
8. https://www.ncsc.gov.uk/news/cyber-experts-warn-of-rising-threat-from-commercial-hacking-tools-over-the-next-five-years#:~:text=Cyber%20experts%20warn%20of%20rising%20threat%20from%20irresponsible%20use%20of,over%20the%20next%20five%20years [↑](#endnote-ref-9)
9. https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html [↑](#endnote-ref-10)
10. https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert [↑](#endnote-ref-11)
11. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/ [↑](#endnote-ref-12)
12. https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/?sh=5ac777d45ed6 [↑](#endnote-ref-13)
13. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/ [↑](#endnote-ref-14)
14. https://www.gov.uk/government/publications/uk-france-joint-leaders-declaration/uk-france-joint-leaders-declaration [↑](#endnote-ref-15)
15. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ [↑](#endnote-ref-16)
16. https://cyberteCybersecurity Tech Accord principles limiting offensive operations in cyberspace [↑](#endnote-ref-20)
17. https://www.business-humanrights.org/en/latest-news/2023-summit-for-democracy-over-45-organisations-call-on-states-to-protect-citizens-against-the-abuse-of-spyware/ [↑](#endnote-ref-21)