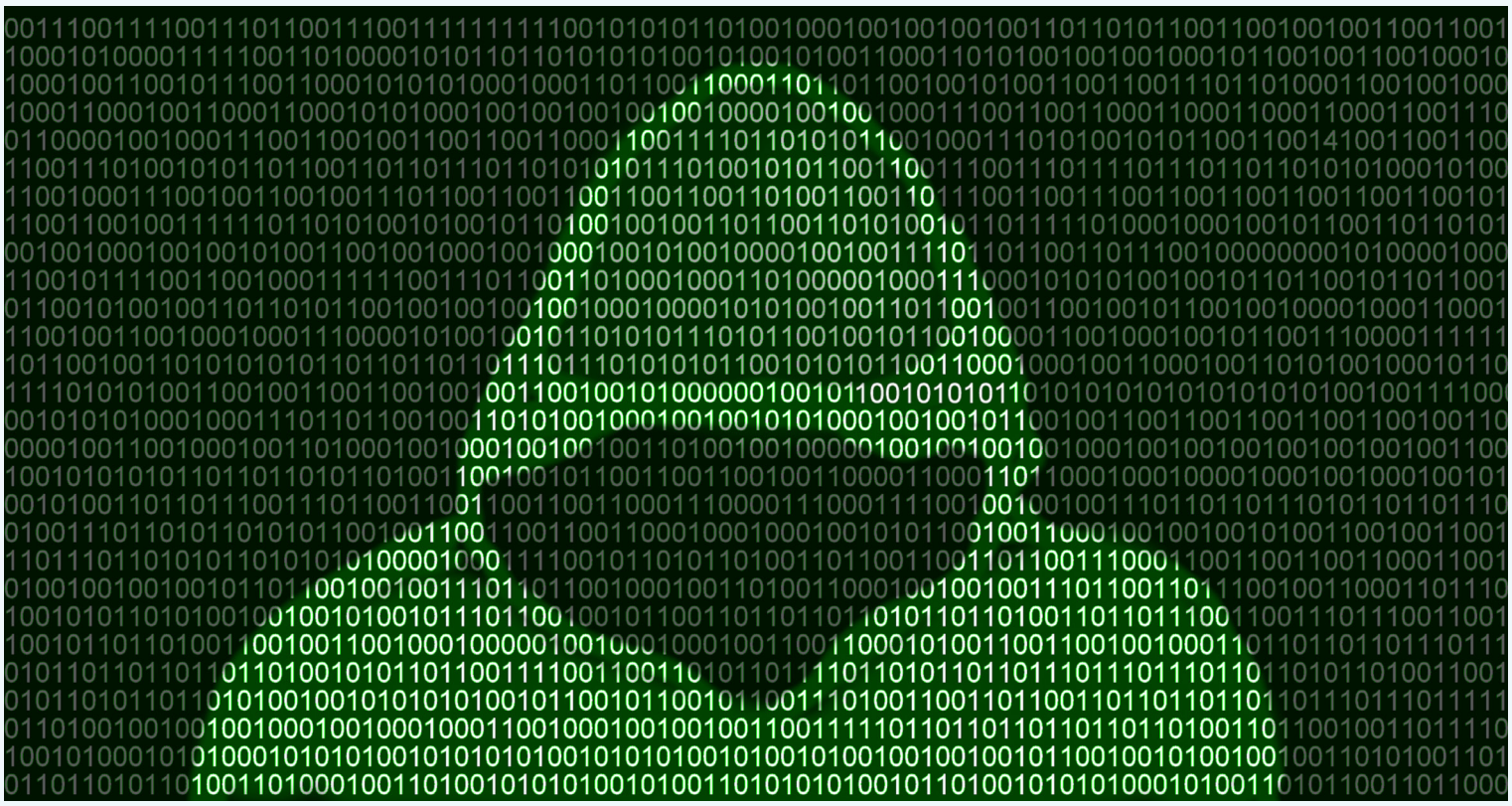
ORF

Chrome Dot Network CDN Series

CYBER MERCENARIES: THE FAILURES OF CURRENT RESPONSES AND THE IMPERATIVE OF INTERNATIONAL COLLABORATION

Fitri Bintang Timur



Attribution: Fitri Bintang Timur, *Cyber Mercenaries: The Failures of Current Responses and the Imperative of International Collaboration*, December 2023, Observer Research Foundation.

This report is part of ORF's Chrome Dot Network initiative. It was produced with support from Microsoft.

Design: Rahil Miya Shaikh
Layout: Simijaison Designs

Cover photo: Getty Images/japatino
Back cover photo: Getty Images/Andriy Onufriyenko

About the Author

Fitriani is a visiting fellow at the International Institute for Strategic Studies Asia-Pacific 2023 and special project researcher at the Centre for Strategic and International Relations. She works on projects related to digital and cyber norms. She is the lead researcher for a study on regional and cross-border responses towards disinformation under the Safer Internet Lab project.

About the Observer Research Foundation

The Observer Research Foundation (ORF) provides non-partisan, independent analyses and inputs on matters of security, strategy, economy, development, energy and global governance to diverse decision-makers (governments, business communities, academia, and civil society). ORF's mandate is to conduct in-depth research, provide inclusive platforms, and invest in tomorrow's thought leaders today.

For more information, visit https://www.orfonline.org/

Contents

Abstract

Digital adoption, hastened globally by the COVID-19 epidemic, brought along with it both benefits and threats, including concerns of safety and security of the cyberspace. Current geopolitical dynamics, ongoing strategic and economic disputes, as well as attempts by authoritarian regimes to preserve power have allowed companies with malicious intent—known as 'cyber mercenaries'—to develop and deploy offensive cyber capabilities. The tools provided by cyber mercenaries are procured and backed by governments to conduct, with plausible deniability, cyber operations that target opposition parties, journalists, civil societies, and even diplomats from conflicting countries; these are often done in gross violation of human rights and jeopardising the safety of the targets. The use of mercenaries in cyberspace is considered as a 'grey-zone' activity due to the absence of agreed international conventions regulating the domain. Technology companies having their products and platforms exploited by cyber mercenaries through 'zero-day' exploits and malicious software, are working together to formulate a joint commitment of Tech Accord Principles in curbing mercenary operations. Similarly, concerned civil society actors have banded together to demand for accountability from mercenary groups supported by governments. Arguably, actions to curb mercenaries can succeed only with the support of national, regional and international standards, as well as the political will and capacity of the concerned governments.

Introduction

INTERNET TRAFFIC REACHED UP TO 60 PERCENT in some countries during the COVID-19 pandemic, as governments responded to the emergency by imposing restrictions on mobility.[1] Despite its advantages, however, digital transformation has also brought about complex problems especially concerning the security of cyberspace as a theatre of strategic contestation. The causes are multiple, and they include the intensifying political, strategic and economic rivalry between United States (US) and China; brewing border contestations—such as the Russia-Ukraine war, the threat of a Taiwan crisis, the Kashmir conflict, and disputes in the South China Sea; as well as insecure authoritarian governments seeking to preserve their rule through any means possible. These tensions are often projected onto the digital space and exploited by criminal groups or companies for their own gain.

There is growing concern that a government's ability to control the cyberspace is eclipsed by the activities of so-called 'cyber mercenaries'—or private entities devoted to creating, promoting and assisting offensive cyber capabilities, and which enable spying on networks, computers, phones, or devices connected by the internet. The 2021 United Nations (UN) General Assembly report has warned that the use of mercenaries in cyberspace[2] could potentially violate the human rights of individuals through methods of data collection, intelligence, and espionage. While these activities are still regarded as 'grey-zone' warfare—and therefore yet to fall under the purview of any formal international agreement—they demand international cooperation.[3]

With the market size of cyber mercenaries passing the US$12-billion mark in 2019[4] and in the absence of an international convention imposing limitations on the matter, the business is only expected to grow. This report expounds on the growing trend of cyber mercenaries and the global developments in addressing the threats. It outlines a set of policy recommendations for setting national and international standards through multi-stakeholder dialogue.

Digital transformation has brought about complex problems concerning the security of cyberspace as a theatre of strategic contestation.

In Search of Definitions: From 'Mercenaries' to 'Cyber mercenaries'

THE TERM 'MERCENARY' has been in existence since the 12th century,[5] and is defined as a person who is recruited, either locally or from overseas, to fight in an armed conflict.[6] Article 47 (2) of the 1997 Additional Protocol to the Geneva Convention of 1949 defines a mercenary as an entity having the motivation to gain financial or material compensation in return for their willingness to fight for the recruiter's country.[7] Arguably, mercenaries are also motivated by ideology, religious conviction, political interest, sense of belonging, and perhaps adventure—which usually develops among youths, the likelihood of individuals and the environment that may perhaps be connected to a violent extremist history.[8]

In the past five years or so, technological advancements have enabled more sophisticated and organised criminal entities who conduct their activities online—or those collectively known as 'cyber mercenaries'.[9] Cyber mercenaries are described as a person, group of persons, or private actors that are hired to carry out cyber offensive or defensive operations to take action on particular cyber networks and infrastructure.[10] They are generally skilled, well-trained entities who have hands-on experience in cutting-edge technologies and are versatile to work on any industry.[11] The recent trend of digitalisation, and the emergence of the Internet of Things (IoT), have created the demand for cyber-skills and knowledge as a service, opening business opportunities both in legal and black markets. Cyber mercenaries are also known as intermediate actors, 'hackers-for-hire', or grey-hat firms.

The wide range of services offered by cyber mercenaries is typically advertised under the rubric of cyber intelligence, digital forensic, pen-testing and information security research, and tech auditing.[12] In private military and security companies (PMCs), cyber mercenaries perform tasks ranging from intelligence gathering, to developing spyware and malware,[13] breadcrumbing data leaks, and even executing distributed denial of service (DDoS or DoS) until the system reaches the desirable degree of information sharing or acceptable failure. Cyber mercenaries also offer destructive services such as damaging industrial systems, undermining a target's information technology prowess, interfering with computers and networks, stealing information, and selling highly sensitive data, including locations and banking information.[14]

Using the services of cyber mercenaries may be useful for state actors to improve their country's cyber warfare capabilities while maintaining some degree of plausible deniability through the avoidance of identification; cyber mercenaries have the ability to launch cyber operations with little or no attribution, thereby shielding their country from the legal consequences or any retaliation.[15] The simplest action is that a state can use cyber mercenaries to collect intelligence or information about their enemies with little repercussions, if at all. When compared to the cost the government must incur to create a new cyber division, hiring cyber-mercenary groups or individuals may be more affordable or cost competitive. This makes employing cyber mercenaries appealing especially for a country that lacks the necessary fiscal, material, technological, and human resources.[16]

A State's choice to employ the services of cyber mercenaries may also be motivated by a certain authority's interest to obtain information for nefarious purposes that is typically directed toward political competitors, human rights activists, journalists, dissidents, and an authoritarian regime's opponents including their families.[17] The operations can manifest, for instance, in remote-controlling the target's personal communication devices, accessing their private images to launch online smear campaigns, extorting from targets, tracking down targeted relatives through information obtained from targets, understanding dissidents' networks, and mounting malicious prosecutions.[18]

Apart from state actors, non-state actors are also prospective clients of cyber mercenaries. It derives from the deployment of cyber-mercenary tools by a government, which can be interpreted as a signal of normalising their use in expanding influence and activities in the digital realm without acquiring the know-how. The absence of a centralised

agency, both in national and international levels, that is mandated to take charge of regulating and coordinating the cyberspace only worsens the problem. As a Startfor Global Analyst publication in 2020 noted, "The absence of a global rule-based system means that the difference in laws, regulations and litigation practices from state to state will only grow as countries try to exert greater control over the Internet."[19] In other words, there is a concern that the lack of both an organising body and transnational legislation hinders the efforts taken by governments, even when they are willing, to defend their country from exploitative online aggressors. Additionally, the uncertain and anarchic nature of international relations has also resulted in the "absence of a global rule-based system" and a central authority, creating an environment where cyber mercenaries thrive.[20] To mitigate the risk of cyber mercenaries to the security of a country or region, it may be beneficial to establish governing regulations on cybercrime activities, including those by cyber-mercenaries, to build assurance in utilising the IoT and information communication technology (ICT). It might also be argued that the demand for cyber mercenaries is aggravated by the increasing level of threats posed by great-power rivalries and sub-regional tensions.

Cyber mercenaries have the ability to launch cyber operations with little or no attribution, thereby shielding their country from the legal consequences or any retaliation.

Cyber mercenaries in the Cybercrime Context

ALL ACTIVITIES UNDERTAKEN BY CYBER MERCENARIES that are against or are violating existing laws can be classified as cybercrime. However, it can be difficult to pinpoint when national legislation is not equipped to handle cyber mercenaries, and the international community has yet to agree on what constitutes cybercrime. For a country not having its own legislation, the treaty commonly used as reference is the 2001 Budapest Convention on Cybercrime—an international legal instrument that facilitates cooperation among its parties to fight cybercrime and hold perpetrators accountable.[21] The Convention provides rules of conduct and standards of acceptable behaviour for the use of the Internet, computers, and related digital technologies; the actions of the public, government, and private organisations; rules of evidence, criminal procedure and other criminal justice matters in cyberspace; and regulation to reduce and/or mitigate the risk of cybercrime targeted towards individuals, organisations, and infrastructure.[22] For some countries, the Budapest Convention on Cybercrime can be a reference point to establish laws to regulate cybercrime; this, however, takes time and resources. Those with limited resources may instead opt to amend their national legislation by adding specific paragraphs and judicial interpretations to apply to existing criminal laws to the digital realm.[23]

In the global context, the UN General Assembly (UNGA) through the work of the Group of Government Experts (GGE), in 2013, recognised that international law applies to states' actions in the cyberspace. Subsequently, the UNGA issued Resolution 70/237 in 2015, which endorses 11 cyber norms of good behaviour in the cyberspace, including preventing misuse of ICT in its territory, cooperating in stopping crime and terrorism, as well as promoting and protecting human rights and privacy on the internet. With the build-up of military capability, there is the concern of future cyberwarfare and, as such, the global community relies on the existing principles of international law, which is reflected in the 2021 GGE report.[24] However, the GGE mechanism that conducted meetings between 2004 and 2021 was criticised for being "exclusive" as the number of participating countries was limited.[25] The UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security was started in 2019 to include all UN Member States and in consultation with businesses and civil societies, with meetings running until 2025 in the current mandate. However, the cyber norms recommended by the UN GGE and OEWG are non-binding and voluntary in nature.

In formulating a binding mechanism for addressing cybercrime, the UN has established an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes in 2021.[26] As it stands, though, there is still no commonly agreed definition of 'cybercrime' and the use of its term. At present, a crime is considered as 'cybercrime' if the perpetrator directs the crime at a computer or other technological devices, or executes illegal conducts with the help of the internet or ICT. The United Nations Office on Drugs and Crime (UNODC)—which serves as secretariat to the Ad Hoc Committee—defines 'cybercrime' as an activity that focuses on the use of a computer system or digital device inherent to the *modus operandi*.[27] Meanwhile, academics like Marcum and Higgins (2019) define cybercrime as the destruction, theft, unauthorised or illegal use, modification or copying of information, programmes, services, equipment or communication network.[28]

From the perspective of protecting individual rights in the digital era, the UN Commission on Human Rights in 2005 established a Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination. In its 2020 report, the Working Group had raised its concerns on the use of new technology, be it by states in engaging in asymmetric conflict, and by private players who seek profit from using it to carry cyber operations to undermine the integrity of another State's territory. The report stated that, "individuals carrying out cyberattacks can be considered as undertaking a mercenary-related activity, or even a mercenary activity if all the qualifying criteria are met."[29] The report calls for appropriate policy and regulatory response from states to make sure that these actors conform to international human rights standards and principles.

As the global architecture is currently structured, governments are the primary duty-bearers obligated to respect, promote and protect human rights. Therefore, there is the expectation for inter-government organisations such as the UN to produce human rights-based frameworks demanding that countries implement transparency when contracting cyber services. Understandably, geopolitical tensions due to US-China competition and the Ukraine-Russia conflict may hamper the adoption, at the UN level, of detailed binding regulations on cybercrime, and the use of cyber mercenaries and offensive cyber capabilities.

With the build-up of military capability, there is the concern of future cyberwarfare; the global community is currently relying on the existing principles of international law.

Notable Use Cases of Cyber mercenaries

THIS PAPER USES THE CASES OF certain infamous activities by cyber mercenaries that have had massive scale and impact: the state-sponsored cyber mercenary Lazarus Group; Advanced Persistent Threat (APT) 32; and the Pegasus spyware. It is important to mention the concerning growth of small and medium impact hack-for-hire services[30] available in the black market. More action is needed to counter such adverse profit-seeking practices.

The first example is "Lazarus", a state-sponsored cyber-mercenary group in North Korea which has been blamed for a number of high-profile cyber-attacks. These include the 2014 Sony Pictures hack, 2016 Bangladesh Bank attack, and the WannaCry ransomware spread in 2017—[31] the last of which affected more than 300,000 computers in 150 countries and made financial gain through theft, extortion, and cryptocurrency-related operations. Though more people were likely to have been involved, in this attack, only one North Korean named Park Jin Hyok was charged for his connection to the government-sponsored hacking team. The Lazarus group affiliates with the North Korean government company, Chosun Expo Joint Venture (or Korea Expo Joint Venture), to back the country's malicious cyber actions.[32] The widespread impact of the group's malicious acts targeting not only government institutions but also critical infrastructure important for civilian lives, such as the hospital system, highlights the importance of having robust cybersecurity measures.

Another cyber-mercenary group known to conduct surveillance is the Ocean Lotus group that deployed the APT 32. Investigations on this APT began in 2018 but it is suspected that it had already been around for a decade then.[33] The targets of APT 32 are governments, network security, technology infrastructure, media, and banking sectors in countries such as Vietnam, the Philippines, the US, and China.[34] This threat actor group utilises a suite of customised malware tools, augmented by commercially available devices inside the targeted network. Targets are not only entities, but individual activists, journalists and dissidents' devices that were penetrated by the malware injected by APT 32 to monitor them on an ongoing basis.

APT 32 is reported to also be targeting the Vietnamese diaspora globally, including those in Australia and appears to have a well-resourced development capability. The threat actor group operates in the area that is deemed to be aligned with the interests of the Vietnamese state, although the interest of the country deploying it is yet to be studied.[35] The motivation of APT 32 seems to be varied in the private sector, who use it for law enforcement, including the prevention of intellectual property theft, or in anti-corruption measures; its application towards individuals is more for threatening political activism and limiting free speech. Similar cyber espionage monitoring was experienced by Cambodia during its 2018 election where the Election Commission, Interior Ministry, diplomats and opposition lawmakers were targeted by the TEMP.Periscope hacking group allegedly working for a neighbouring country that had vested interest on the country's election results.[36]

Another group that has caught media attention is the Israel-based NSO. The private firm, which owns cyber tools with the power to conduct mass surveillance, produced the Pegasus spyware in 2011.[37] Until 2018, the tool had been bought by at least 45 countries across the globe, to conduct national and cross-border surveillance operations on the cell phones of civil society activists, monitoring their activities and communications.[38] The Pegasus spyware shares information from the infected cell phone with the operator that plants the spyware: calls, text messages, contact details, microphone recordings, photos, screenshots, files, calendar records, location tracking, and browsing history.

Countries that are suspected to have experienced tracking by Pegasus include Canada, India, Pakistan, Singapore, Thailand, and the United States. In August 2016, after the initial reports about the spyware emerged, the NSO Group published a statement noting that the company complies with relevant laws and does not operate the software for clients, only develops it, which therefore hands the responsibility of the use of the tool to the governments who buy it.[39] Pegasus is referenced in the 2021 report by UNCHR established Working Group on the use of mercenaries, as a company that benefits from the rapidly growing market of offensive cyber capabilities that is "subject to little regulations and has the opportunity to make significant profit."[40]

Yet it is not only the NSO Group that has engaged in such activities. Other companies, such as the Atlas Intelligence Group suspected of having a base in a European country,[41] have created a cyber-army division to conduct digital information operations, such as data leaking, DDoS, server take-down, remote-desk protocol/control, panel hacking to providing initial access to desired target networks with relatively affordable starting cost of US$20 for US$1,000.[42] Meanwhile, the international community has yet to set any binding framework[43] to address the increasing threat of cyber mercenaries and outline the legal responsibilities of states or private actors in procuring and utilising their tools and services in ways that violate human rights.

Following the revelation about Pegasus, countries are switching to the use of similar spyware tools. One of the replacements is Predator, produced by Cytrox, a subsidiary of EU-based Intellexa and is knowingly deployed by the governments of Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia.[44] Intellexa's website audaciously calls itself a "regulated company" despite producing spyware used for hacking and violating privacy rights, revealing a loophole in the national and international regulations tech space.

More action is needed to counter the adverse profit-seeking practices of cyber mercenaries.

As Governments Become the Market, Companies Prevail

FOR STATE ACTORS, EMPLOYING CYBER MERCENARIES is useful for conducting offensive cyber operations as they provide plausible deniability while achieving their objectives which can range from maintaining national power to asserting influence on other states. According to 2023 data from the Carnegie Endowment for International Peace, at least 74 countries deployed spyware or digital forensics technology procured from commercial firms and applied them on more than 190 counts.[45] This number is an increase from around 40 countries employing such tools in 2015[46] and 65 countries in 2020.[47] With more governments procuring cyber-mercenary services, these companies have virtually become extensions of state power, able to operate beyond the boundaries of human rights and ethics.

To be sure, however, not all companies are willing accomplices. In an effort to protect their brand and consumers' trust, notable ICT companies have vowed to safeguard their users from cybersecurity risks by committing to act responsibly, to empower their users and customers, and thereby aim to improve the security, stability, and resilience of cyberspace. In 2018, 34 companies committed to deliver integrity work to protect users from malicious attacks in four areas: stronger defence, no offense, capacity building, and collective action under the Cybersecurity Tech Accord.[48] The number of signatories to the Accord has grown to 156 companies globally,[49] reflecting the desire and willingness of industries to work for the common good of securing the online environment.

Despite the 2018 Tech Accord, however, specific concerns around governments procuring offensive cyber tools from profit-seeking entities have not been addressed, and companies are finding their own ways to tackle it. For example, in 2019, Facebook alerted almost 50,000 of its account holders that they had been targeted by surveillance-for-hire mercenaries.[50] Similarly, Microsoft published the results of its own investigation on private sector offensive actors in 2021, saying Israel-based company Candiru "sells cyberweapons that enable its customers, often government agencies around the world, to hack into their targets' computers, phones, network infrastructure and devices connected to the Internet."[51] According to Microsoft, the victims were located in Israel, Iran, Lebanon, Yemen, Spain, the United Kingdom, Turkey, Armenia, and Singapore. In 2023, the Tech Accord issued principles to address cyber mercenaries through five good practice commitments: (1) take steps to counter cyber mercenaries' use of products and services to harm people; (2) identify ways to actively counter the growing cyber mercenary market; (3) invest in cybersecurity awareness of customers, users and the general public; (4) protect customers and users by maintaining the integrity and security of products and services; and (5) develop processes for handling valid legal requests for information.[52]

The Tech Accord Cyber-Mercenary was co-authored by major ICT companies whose products were being exploited by mercenaries as launch pads for attacks—i.e., Cisco, Meta, Microsoft, and Trend Micro; as of March 2023, the accord has gathered support from 40 companies.[53] It remains to be seen, however, if the pledge will succeed in supporting the protection and promotion of human rights principles. The reality is that these pro-human-rights companies need to navigate applicable laws, government restrictions, internal policies and processes to maintain profits for their shareholders, which may constrain their ability to address the threat of cyber mercenaries.

Meanwhile, for cyber mercenaries, the market is relatively barrier-free with high demand for intrusion technology that financially motivates them to maintain their presence.[54] They are also economically articulate to exploit regulatory fragmentation. For example, the Israel-based NSO Group established subsidiaries in Bulgaria and Cyprus, while Intellexa is operating in six research sites throughout Europe. At the same time, states are not the only actors who procure services of cyber mercenaries, as non-state actors can similarly employ them. However, as primary duty bearers of human rights and to protect their sovereignty, states need to be aware of the cyber security risks in allowing the presence of cyber mercenaries.

Going Forward: Multistakeholder Action

GOVERNMENTS NEED TO BE AWARE of the grave reputational risks in employing and allowing cyber mercenaries to operate in their territory and supporting the market for their presence. Civil society organisations such as Citizen Lab and Amnesty International's Security Lab have published updates on the cyber-mercenary ecosystem since the early 2010s. These reports are game changers as they provide ammunition for pressure groups to demand governments to address the issue of cyber mercenaries. For example, after Citizen Lab published its 2015 report on Germany-based FinFisher that exported spyware to countries with serious human rights violations,[55] in 2019, the coalition of Society for Civil Rights (GFF), Reporters Without Borders Germany (RSF Germany), the European Centre for Constitutional and Human Rights (ECCHR), and the blog Netzpolitik.org filed a legal suit against FinFisher. The following year, the police raided FinFisher's office in Munich and the court ceased its business operations in 2022.[56] This kind of pushback from civil society against mercenary companies is only possible in the European Union (EU), after the issuance in 2015 of regulation requiring governments to authorise the export of surveillance software.

Discussions on addressing the issue of cyber mercenaries, specifically the employment of spyware, took place in the EU in 2021 after the governments of member countries were reported to be deploying Pegasus and other similar software among journalists and political opponents, including those in Estonia, Hungary, Spain and Greece.[57] Additionally, EU leaders, such as the European Council President Charles Michel and French President Emmanuel Macron were reportedly being targeted by spyware from a Moroccan client.[58] To provide warning on these findings, the European Data Protection Supervisor (EDPS) stated in public reminders that the deployment of highly intrusive spyware technology is not compatible with the EU legal order.[59] It also recommended stricter conditions and safeguards to be implemented on the export and also import of intrusive surveillance technologies, to allow for background checks on dubious companies entering the EU territory. For its part, the EU Commission was not in favour of investigating member states' use of Pegasus spyware, regarding such decision as part of "national security" and thereby leaving the states themselves to the responsibility.[60]

To effectively govern the cyberspace, countries and regions need to be willing and have the regulatory capacity to do so. Using the same argument of protecting national interest but in an opposing manner, in 2021 the US included the NSO Group and Candiru to its Entity List, blacklisting these companies after they developed and supplied tools maliciously targeting government officials, journalists, businesspeople, activists, academics, and embassy workers.[61] Under the same regulation, Russia-based Positive Technology and Singapore-listed Computer Security Initiative Consultancy PTE Ltd were also added to the List due to their work in cyber traffic tools used to gain unauthorised access of information systems.

Two years later, in March 2023, US President Joe Biden issued an Executive Order that prohibited government use of commercial spyware due to concerns of counterintelligence security risk.[62] The regulation was issued after it was revealed that the cell phones of diplomats at the US Embassies in Kenya and Uganda were hacked using the Pegasus software. Meanwhile, Israel stated that the NSO Group software is a crucial part of foreign policy and lobbied the US to take Pegasus out of the negative list, noting that the abilities to remotely and discreetly penetrate devices, monitor locations, and extract their content would be helpful in combatting global organised crime and terrorism.[63] If its request is granted, Israel will commit to implement tighter software licensing for prospective clients of the NSO Group.[64] If the company is not removed from the black list, then the blacklisted company may fall into bankruptcy and be driven out of the market, although the experts behind the Group may easily transfer their skills elsewhere or open another company offering similar services.

Conclusion

COOPERATION AMONG NATIONS, both within a region and globally, is crucial to enhance cybersecurity resilience and safeguard against cyber threats, including those posed by cyber mercenaries. Admittedly, there are governments that actively employ cyber mercenaries due to the latter's ability to execute highly skilled cyber operations whilst maintaining plausible deniability. This is especially noticeable for countries with internal political disputes, authoritarian regimes, problematic human rights records, or are in conflict with other countries.

Nevertheless, peaceful countries such as the EU member states also harbour cyber-mercenary subsidiaries and research centres due to loopholes in their respective legislations. Many governments procure mercenary services under the pretext of protecting national security although tools used by mercenaries may be counterintuitive as clients' information can be leaked by unprincipled companies to the highest bidder. Having a national cyber legislation that includes regulation on the use of cyber intelligence and digital forensic tools would be beneficial to ensure that their usage adheres to human rights and values. Standards must be set so that acts that purportedly protect national security should also respect the Universal Declaration on Human Rights and other human rights declarations.

While such standards are being formulated through international negotiations at the UN, including through GGE, OEWG and the drafting of the Cybercrime Convention, the private sector plays a significant role in regulating the market and running technological platforms. The document, Tech Accord Principles to Curb Cyber Mercenaries, has shown the commitment of industries to support the maintenance of safety and security in cyberspace. The ICT companies have the ability to limit the movement of cyber mercenaries by identifying and disrupting the use of tools employed by them on the companies' platforms, documenting and reporting the groups, and initiating legal action against them.

Civil society groups have taken action by filing legal suits to demand for transparency on government-backed entities working as cyber mercenaries. Citizens, through media and civil society organisations, must demand accountability from governments and businesses in their activities of applying and marketing technological products and services. This is so that the citizens' economic and political rights, including the right to privacy and free speech, are protected. The existing Tech Accord, industry principles, and civil society legal proceedings have provided benchmarks for responsible behaviour in the cyberspace. The hope is that these will ignite multi-stakeholder discussions between governments, businesses and civil societies to call for action in addressing, or even banning, cyber mercenaries.

Endnotes

1 Organisation for Economic Co-operation and Development (OECD), *Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides*, (Paris: OECD, 2020), https://www.oecd.org/digital/digital-economy-outlook-covid.pdf

2 UN General Assembly Document, *Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, No. A/76/151, July 15, 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/192/08/PDF/N2119208.pdf?OpenElement

3 Kohei Takahashi et al., *Building Cooperation: Cyber, Critical Technology and National Security*, (Canberra: Quad Tech Network Series, 2021), p. 1, https://nsc.crawford.anu.edu.au/publication/18424/building-cooperation-cyber-critical-technology-and-national-security

4 Mark Mazzetti, et al., "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments," *New York Times*, March 21, 2019, https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html

5 Sarah Percy, "Mercenaries", *Oxford Bibliographies*, 2023, https://www.oxfordbibliographies.com/view/document/obo-9780199791279/obo-9780199791279-0105.xml

6 United Nations Office of the High Commissioner for Human Rights (OHCHR), *Visit to Austria: Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, document number A/HRC/42/42/Add.2, (Geneva: OHCHR, 2019), https://www.ohchr.org/en/documents/country-reports/ahrc4242add2-visit-austria-report-working-group-use-mercenaries-means

7 Martina Gasser and Mareva Malzacher, "Beyond Banning Mercenaries: The Use of Private Military and Security Companies Under International Humanitarian Law," *Journal of International Humanitarian Law and Non-State Actors, (*2019), pp. 47-77, https://link.springer.com/chapter/10.1007/978-94-6265-339-9_3

8 United Nations OHCHR, *Visit to Austria*.

9 Although the concern of mercenary-like activities of intrusion to computer system has been reported since 2013 by the United Kingdom Intelligence Service Annual Report, the cases directed to individuals were reported since 2019. UK Intelligence and Security Committee of Parliament, *Annual Report 2012–2013*, 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211553/31176_HC_547_ISC.PDF and Citizen Lab, NSO Group / Q Cyber Technologies, October 29, 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

10 Miles Kenyon, *Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries,* 2021, https://citizenlab.ca/2021/02/citizen-lab-response-to-the-u-n-working-group-on-the-use-of-mercenaries/

11 Lorenzo Valeri, "The Information Warrior," *Journal of Financial Crime*. 6, No. 1 (1998), pp. 52-53*,* https://www.emerald.com/insight/content/doi/10.1108/eb025862/full/html?skipTracking=true

12 Raphael Satter and Christopher Bing, "How mercenary hackers sway litigation battles," *Reuters*, June 30, 2022, https://www.reuters.com/investigates/special-report/usa-hackers-litigation/

13 Amnesty International, *Hackers For-hire in West Africa Activist in Togo Attacked with Indian-made Spyware,* 2021, https://www.amnesty.org/en/documents/afr57/4756/2021/en

14 Feike Hacquebord, *Void Balaur: Tracking a Cybermercenary's Activities,* (Texas: Trend Micro Research, 2021), https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf

15 Janine Schmoldt, *The Rising Power of Cyber Proxies* (paper presented at the European Conference on Cyber

Warfare and Security, the United Kingdom, June 2021), https://www.proquest.com/docview/2555179801/abstract/9936285F27784EBDPQ/1?accountid=31495

16 Emilio Iasiello, *The Cyber Mercenary Business is Booming*, OODALOOP, 2022, https://www.oodaloop.com/archive/2022/08/02/the-cyber-mercenary-business-is-booming/

17 Kenyon, *Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries*

18 Kenyon, *Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries*

19 José Arimatéia da Cruz and Stephanie Pedron, "Cyber Mercenaries: A New Threat to National Security," *International Social Science Review*, 96 (2020), https://www.proquest.com/docview/2429820539?pq-origsite=gscholar&fromopenview=true

20 Cruz and Pedron, *Cyber Mercenaries*

21 US Department of Justice, *United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime*, Washington DC, 2022, https://www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat.

22 United Nations of Office on Drugs and Crime (UNODC), "The Role of Cybercrime Law," *Teaching Module Series*, (Vienna: UNODC, 2017), https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

23 UNODC, "The Role of Cybercrime Law"

24 Bart Hoogeven, "The Future of Cyberwarfare in the Indo-Pacific," *ORF Issue Brief*, January 2023, https://www.orfonline.org/wp-content/uploads/2023/01/ORF_IB-604_Future-of-Cyber-Warfare-in-the-Indo-Pacific.pdf

25 Elaine Korzak, "Russia's Cyber Policy Efforts in the United Nations," *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Tallinn Paper*, 2021, No. 11, https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf; Heli Tiirmaa-Klaar, "The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body," *Cyberstability Paper Series*, December 2021, https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf

26 Ian Tennant and Summer Walker, "UN Cybercrime Treaty Ad Hoc Committee," *Global Initiative Article*, May 8, 2023, https://globalinitiative.net/analysis/international-convention-ict-crime-ahc-un-2/

27 United Nations Office on Drugs and Crime, *Computer-related offences*, https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/computer-related-offences.html

28 Catherine Marcum and George Higgins, "Cybercrime", in Marvin Krohn, et al., *Handbook on Crime and Deviance,* (Switzerland: Springer Nature, 2019), pp. 459-475.

29 UN General Assembly, *Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, Document No. A/75/259, July 28, 2020, https://digitallibrary.un.org/record/3883092/files/A_75_259-EN.pdf

30 Danny Palmer, "Cybersecurity: This Prolific Hacker-for-Hire Operation has Targeted Thousands of Victims Around the World," *ZDNET*, November 10, 2021, https://www.zdnet.com/article/this-cyber-mercenary-hacking-group-has-targeted-thousands-of-victims-around-the-world/; Franz Wild, et al., "Inside the Global Hack-for-Hire Industry," *The Bureau of Investigative Journalism*, November 5, 2022, https://www.thebureauinvestigates.com/stories/2022-11-05/inside-the-global-hack-for-hire-industry

31 BBC, "The Lazarus Heist: How North Korea Almost Pulled Off a Billion-Dollar Hack," *BBC News*, June 21, 2021, https://www.bbc.com/news/stories-57520169

32 US Department of Justice, “North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions,” *US Department of Justice Press Release*, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

33 Symantec Threat Hunter Team, “Billbug: State-sponsored Actor Targets Cert Authority, Government Agencies in Multiple Asian Countries,” *Symantec Enterprise Threat Intelligence*, November 15, 2022, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority

34 Nick Carr, *Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations*, (Virginia: Mandiant, 2017), https://www.mandiant.com/resources/blog/cyber-espionage-apt32

35 Carr, *Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations;* Bug Crowd, “APT 32”, 2023, https://www.bugcrowd.com/glossary/apt32/

36 Abby Seiff, “Chinese State-Linked Hackers in Large Scale Operation to Monitor Cambodia's Upcoming Elections, Report Says,” *Time*, July 10, 2018, https://time.com/5334262/chinese-hackers-cambodia-elections-report/

37 Neri Zilber, “The Rise of the Cyber-Mercenaries,” *Foreign Policy*, August 31, 2018, https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/

38 Bill Marczak, *Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries*, (Toronto: Citizen Lab, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

39 TOI Staff, “Israeli government okayed sale of spyware that exploits iPhones,” *Times of Israel,* September 7, 2016, https://www.timesofisrael.com/israeli-government-okayed-sale-of-spyware-that-exploits-iphones/

40 UN General Assembly, *Use of Mercenaries as a Means of Violating Human Rights and Impeding The Exercise Of The Right Of Peoples To Self-Determination*, Document No. A/76/151, July 15, 2021, https://digitallibrary.un.org/record/3953993?ln=en

41 Ethan Freedman, "Israeli cyber intel firm shines bright light on new, shadowy cybercrime collective," *Times of Israel*, October 20, 2022, https://www.timesofisrael.com/israeli-cyber-intel-firm-shines-bright-light-on-new-shadowy-cybercrime-collective/

42 Shmuel Gihon, “Atlas Intelligence Group (A.I.G) – The Wrath of a Titan,” *Cyber Intelligence*, July 20, 2022, https://cyberint.com/blog/research/atlas-intelligence-group/

43 Peter Micek, “The Proliferation of Cyber Mercenaries Calls for New Definitions and Updated Laws,” *Foreign Policy Analytics*, 18 August 2023, https://digitalfrontlines.io/2023/08/18/the-proliferation-of-cyber-mercenaries-calls-for-new-definitions-and-updated-laws/

44 Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert, *Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, (Toronto: Citizen Lab, 2021), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

45 Steven Feldstein and Brian Kot, Global Inventory of Commercial Spyware & Digital Forensics in the Mendeley Data, March 2023, https://data.mendeley.com/datasets/csvhpkt8tm/10

46 Lorenzo Franceschi-Bicchierai, “Hacking Team Founder: ‘Hacking Team is Dead’,” *The Vice*, May 27, 2020, https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead

47 Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, (New York: Oxford University Press, 2021); Steven Feldstein and Brian, “Governments Are Using Spyware on Citizens. Can They Be Stopped?,” *Carnegie Endowment for International Peace*, July 21, 2021, https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

48 Tech Accord, “Signing pledge to fight cyberattacks, 34 leading companies promise equal protection for customers worldwide,” *Tech Accord News*, April 17, 2018, https://cybertechaccord.org/signing-pledge-to-fight-attacks-cyber-accord/

49 Tech Accord, *Signatories*, July 2023, https://cybertechaccord.org/signatories/

50 Stephanie Kirchgaessner and Michael Safi, “Facebook bans seven ‘cyber mercenary’ companies from its platforms,” *The Guardian*, December 16, 2021, https://www.theguardian.com/technology/2021/dec/16/facebook-bans-surveillance-companies-warnings-malicious-activity

51 Christin Goodwin, “Fighting cyberweapons built by private businesses,” *Microsoft Blogs*, July 15, 2021, https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/

52 Tech Accord, “Cyber mercenaries: An old business model, a modern threat,” *Principles*, March 2023, https://cybertechaccord.org/uploads/prod/2023/03/Cyber-mercenary-principles_Tech-Accord_032723_FINAL.pdf

53 Tech Accord, “Cyber mercenaries”

54 Steven Feldstein and Brian Chun Hey Kot, “Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses,” *Carnegie Endowment for International Peace*, March 14, 2023, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

55 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, *Pay No Attention to the Server Behind the Proxy*, (Toronto: Citizen Lab, 2015), https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

56 European Center for Constitutional and Human Rights (ECCHR), Criminal Complaint Against Illegal Export of Surveillance Software is Making an Impact, March 28, 2022, https://www.ecchr.eu/en/press-release/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact/#:~:text=Following%20a%20criminal%20complaint%20filed,based%20corporate%20group%20FinFisher%20has

57 European Parliament, *Investigation of the Use of Pegasus and Equivalent Surveillance Spyware*, June 7, 2023, https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)747923 and Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, REPORT of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 2022, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf

58 European Parliament, *Pegasus and Surveillance Spyware*, (Brussels: European Parliament, 2022), https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

59 European Data Protection Supervisor, *EDPS Preliminary Remarks on Modern Spyware*, February 15, 2022, https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en

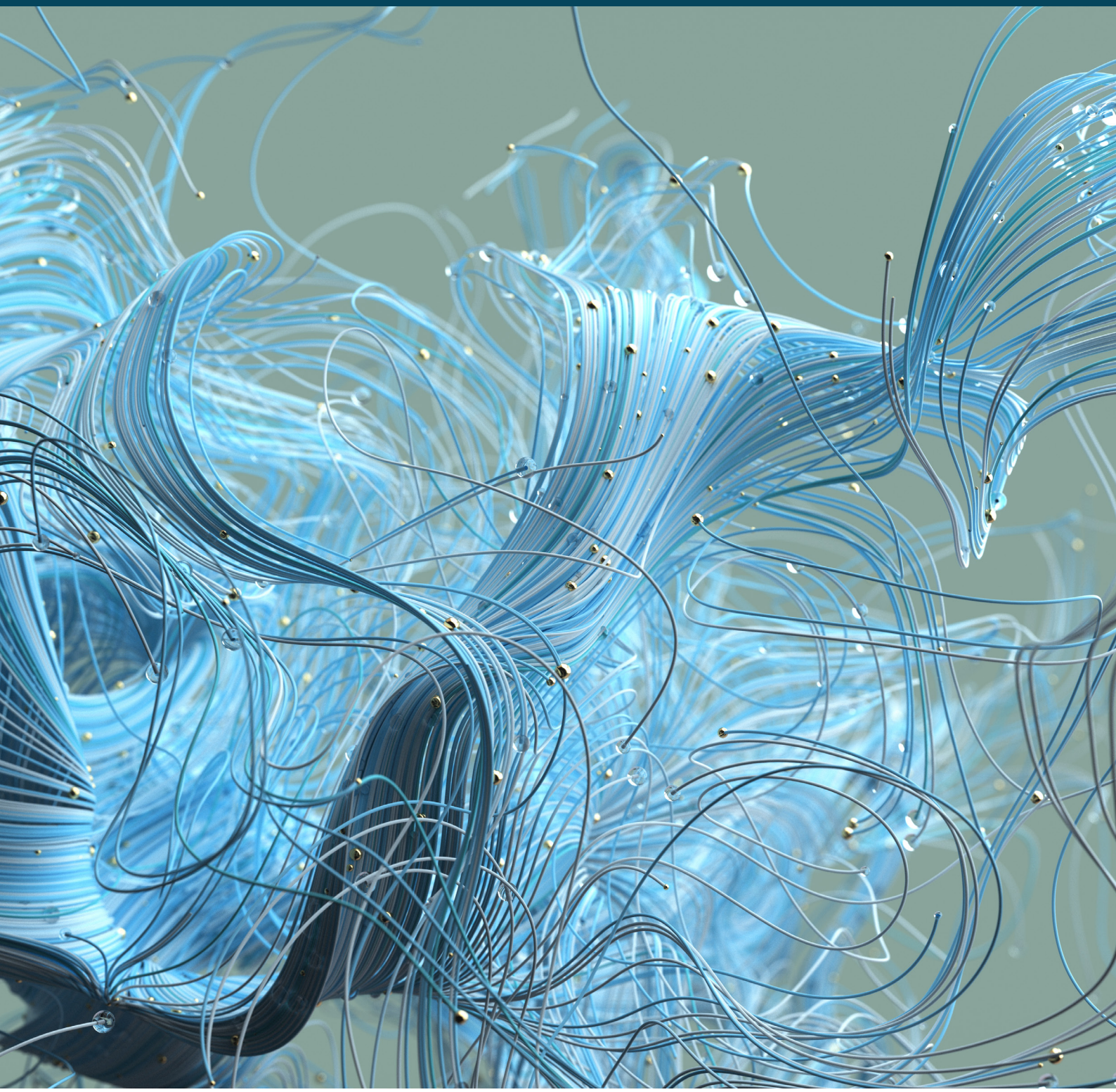
60 Nikolaj Nielsen, “EU Commission Won't Probe 'Pegasus' Spyware Abuse,” *EU Observer*, April 19, 2022, https://euobserver.com/digital/154752

61 US Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, Washington DC, November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

62 White House, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, Washington DC, March 27, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

63 Ronen Bergman and Patrick Kingsley, “Despite Abuses of NSO Spyware, Israel Will Lobby U.S. to Defend It,” *New York Times*, November 8, 2021, https://www.nytimes.com/2021/11/08/world/middleeast/nso-israel-palestinians-spyware.html

64 Peter Beaumont and Philip Oltermann, "Israel to Examine Whether Spyware Export Rules Should be Tightened," *The Guardian*, July 23, 2021, https://www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus



ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area
New Delhi - 110 002, INDIA
+91-11-35332000 Fax: +91-11-35332005
contactus@orfonline.org
www.orfonline.org