Research Paper

International Security Programme

October 2024

Principles for state approaches to commercial cyber intrusion capabilities

Navigating the policy challenges of cyber intrusion markets

James Shires

11:54

ALERT: State-sponsored attackers may be...

If you've previously received a threat notification from Apple, this additional notice is to inform you that we believe new or continued targeting has occurred.

Apple recommends that you immediately take these actions:

- Update your iPhone to the latest software version, iOS 17.1, if you haven't already. We urge you to always update to the latest software as soon as it's available, as it contains the latest security protections. To update, go to Settings > General > Software Update.

CHATHAM HOUSE

European Cyber Conflict Research Incubator

RUSI

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- Cyber intrusion – the ability to access and manipulate a digital device, system or network remotely and without proper authorization – has become commercialized. The scale at which cyber intrusion capabilities are now available is largely due to rapid growth of the markets in which such capabilities and their component parts can be bought and sold as products and services by states, companies and criminals.

- In addition to their use by cybercriminals, many states, including military and intelligence agencies, have turned to the commercial acquisition of such capabilities as an alternative to developing and maintaining them in-house. But states frequently use such capabilities in ways that violate international human rights law or otherwise undermine norms of responsible state behaviour.

- In recent years, civil society, industry and state actors have proposed a wide range of policy interventions to counter the proliferation and misuse of commercial cyber intrusion capabilities. However, existing interventions are focused mainly on a narrow group of states and specific issues. As a result, they risk incoherence and inconsistency, and are unlikely to encourage substantive change across the whole landscape.

- This paper suggests principles for state approaches to shaping the market for commercial cyber intrusion capabilities, both promoting their responsible use and countering their irresponsible use. Principles can help disparate interventions achieve consensus from multiple perspectives, from narrow national security objectives to broader concerns regarding human rights or the security of the internet architecture. They can also help to identify opportunities for high-level agreement on aims despite disagreement on specific use cases, moving beyond centres of existing regulation in the US and Europe.

- The principles are underpinned by a new distinction between ‘permissioned’ and ‘unpermissioned’ intrusion. Permissioned intrusion takes place with the permission of either the user, the owner or the operator of a targeted device, system or network. Unpermissioned intrusion, as the term suggests, takes place without at least one of these permissions.

- This distinction is important because it moves the focus of debate away from the contested application of concepts of ‘legitimacy’ and ‘dual use’, towards a clearer test of permission. The aim is to minimize concerns over the impact of regulation and policy on genuine cybersecurity research and testing practices – an issue that has stymied many previous high-profile interventions –

as well as to reduce confusion between different kinds of legitimacy (such as that of a government intelligence agency versus that of a client of a security testing service).

- The principles are summarized as follows:

  1. States should align their approaches across markets for commercial cyber intrusion capabilities, including as customers and users, investors, detectors and defenders, and regulators.

  2. States should separate markets for permissioned cyber intrusion from markets for unpermissioned cyber intrusion as far as possible: administratively, legally and technologically.

  3. States should stimulate markets for permissioned use of commercial cyber intrusion capabilities.

  4. States should not engage commercial actors to independently conduct unpermissioned cyber intrusion on their behalf.

  5. States should be transparent in acknowledging unpermissioned cyber intrusion for military, national security and law enforcement purposes.

  6. States should integrate their practices of unpermissioned intrusion with their efforts to improve anti-corruption, security governance and rule of law.

  7. States should adopt OECD principles for government access to data, along with UN norms of responsible state behaviour, as minimum standards in their practices of unpermissioned intrusion.

  8. States should apply, at a minimum, equally high standards to internal development and interstate transfer as they do to commercial activities.

- Ultimately, widespread adoption of these principles by states would mean commercial cyber intrusion capabilities are sourced in a more restrained and responsible way. Such capabilities would be only used by states, and then only when meeting clear thresholds of necessity and proportionality and in ways compatible with international law – including international human rights law.

01 Introduction

The rapid growth of markets in which cyber intrusion capabilities can be bought and sold as products and services by states, companies and criminals raises thorny policy challenges. This paper explores these challenges, and puts forward a set of principles to help governments and wider society navigate commercial markets for cyber intrusion technologies.

Cyber intrusion capabilities – the ability to access and manipulate a digital device, system or network remotely and without authorization – are becoming globally and easily available to state and many non-state actors. These capabilities are, simultaneously, a crucial means of testing and improving digital defences, a troubling new vector for fraud, ransom demands and other criminal activity, and an integral aspect of contemporary statecraft and military power. For example, cyber intrusion capabilities help law enforcement agencies to track criminals, but also help criminals obtain their victims' data; and they help states to conduct cyber espionage while also helping organizations bolster their digital defences against such espionage.

The scale at which cyber intrusion capabilities are available is largely due to rapid growth of the markets in which such capabilities – and their component parts – can be bought and sold as products and services by states, companies and criminals. Simply put, cyber intrusion has become commercialized.

The commercialization of cyber intrusion capabilities raises thorny policy challenges. Market-driven efficiencies emerging organically from an increasing division of labour and role specialization in cybercriminal groups have greatly increased the threat of ransomware attacks, hack-and-leak operations and digital fraud for individuals, organizations and countries worldwide. At the same time, the wealth of information now contained on people's devices, collected by companies and governments, and stored in cloud data centres, makes cyber intrusion a highly attractive vector for state intelligence collection. Many countries have turned to the commercial acquisition of cyber intrusion capabilities as an alternative to developing and maintaining them in-house (i.e. within their own military, intelligence or law enforcement bodies). But many states have used such capabilities in ways that violate international human rights law – including by targeting journalists, political opposition and civil society activists without meeting legal requirements such as necessity and proportionality – or that otherwise undermine norms of responsible state behaviour in cyberspace.

This paper puts forward principles for state approaches to commercial cyber intrusion capabilities. It is aimed primarily at government policymakers in this area, but is intended also for the use of other critical stakeholders, from civil society organizations to government practitioners, and from the cybersecurity industry to individual hackers.

The wealth of information now contained on people's devices, collected by companies and governments, and stored in cloud data centres, makes cyber intrusion a highly attractive vector for state intelligence collection.

The research that has informed the paper is funded by the UK Foreign, Commonwealth and Development Office, in parallel with the Pall Mall Process led by the UK and France. Importantly, however, the principles set out in the paper are offered to the debate on commercial cyber intrusion capabilities as an independent product of research conducted by the cyber policy team within the Chatham House International Security Programme. The views expressed are solely those of the author, and not of any governments or other stakeholders supporting or otherwise involved in the research. The principles are intended to contribute to existing thinking among governments and wider society about how to shape the market for commercial cyber intrusion capabilities; and through this contribution also constitute an argument for a multi-stakeholder approach to governance in this area.

Next, Chapter 2 introduces the key distinction, which underpins the paper, between permissioned and unpermissioned uses of commercial cyber intrusion capabilities. Chapter 3 provides a summary of relevant existing interventions. Chapter 4 explains why the paper focuses on principles rather than other kinds of intervention such as regulation. Chapter 5 summarizes key themes emerging from a workshop at which stakeholders from multiple disciplines discussed an earlier draft of the principles introduced in this paper. Chapter 6 sets out the principles themselves. In conclusion, Chapter 7 offers a prognosis regarding the future development of the markets underlying permissioned and unpermissioned intrusion.

02 Permissioned and unpermissioned cyber intrusion

Existing concepts of legitimate and illegitimate use do not adequately address the complexities of the challenges states now face concerning cyber intrusion markets. In an effort to move the debate forward, the principles introduced in the paper are underpinned by a fresh distinction between 'permissioned' and 'unpermissioned' intrusion.

At the root of the challenges described in the previous chapter is what is usually termed the 'dual use' nature of cyber intrusion capabilities and their component parts. However, the 'dual use' label is itself unhelpful in this context. 'Dual use' commonly refers to distinct military and civilian uses, which certainly applies to cyber intrusion capabilities. But in relation to cyber intrusion capabilities, 'dual use' also refers to a wider distinction between legitimate and illegitimate use. There is, however, extensive disagreement about what counts as a legitimate use; and this is especially so in the realm of intelligence collection, where the use of commercial cyber intrusion capabilities against individuals and organizations is usually authorized by governments according to national laws and procedures. This disagreement lies at the heart of most policy debates on the matter, with different stakeholders, such as civil society, governments and the cybersecurity industry tending to talk past one another: what some see as a clear malicious hack, others see as a legitimate state intelligence operation.

Such deep differences are also evident in the characterization of the problem overall as one of either proliferation or misuse. In line with nuclear and other weapons policy arenas, the proliferation characterization suggests that the key issue is the spread of commercial cyber intrusion capabilities beyond their 'legitimate' users – whether to cybercriminals or beyond a certain group of states. In contrast, the misuse characterization suggests that the possession (and purchase) of such capabilities is not in itself an issue; instead, it is 'illegitimate' *uses*, not a greater number of users, that are the primary concern. Although these two framings are clearly connected, the distinction matters for policy responses. In a proliferation framing, the goal is to limit the growth of the market; in a misuse framing, the goal is to steer the market (of whatever size) away from certain kinds of use.

This paper offers a fresh perspective on the debate concerning cyber intrusion capabilities by moving away from concepts of dual or legitimate versus illegitimate use. Instead, it draws an important distinction between 'permissioned' and 'unpermissioned' intrusion.

Permissioned intrusion takes place with the permission of the user, owner or operator of a relevant device, system or network. Unpermissioned intrusion takes place, as the term suggests, without at least one of these permissions.

Inevitably for such a complex subject, both terms include a wide variety of activity. The paradigmatic case of permissioned intrusion is cybersecurity-focused activities such as red-teaming and penetration testing.[1] Unpermissioned intrusion, in contrast, encompasses a wide range of activities from law enforcement takedowns of cybercrime infrastructure and the capture of evidence for arrests of exploiters of minors, to cybercriminal ransomware, corporate espionage and surveillance of journalists.

This new distinction between permissioned and unpermissioned intrusion is important because it moves the focus of debate away from what is or is not a legitimate state use of cyber intrusion capabilities. Rather than dividing uses down a highly contentious line of legitimacy, it instead seeks to ringfence uses on which there is a great deal of – albeit not total – agreement that these should be supported and encouraged (i.e. permissioned uses).

Ultimately, the aim is to minimize concerns over the impact on permissioned uses of regulation and policy concerning unpermissioned uses. This is an issue that has stymied many previous high-profile interventions, including various attempts by states to introduce export controls into their domestic legislation (discussed in more detail in the next chapter).

As a pair, the terms permissioned and unpermissioned are also useful precisely because they are not already prevalent. For example, the terms authorized and unauthorized [cyber intrusion] could arguably be used in the same way as permissioned/unpermissioned in this paper. However, lack of 'proper' authorization is – as noted above – often part of the definition of intrusion itself, and the term is also frequently used in the context of law enforcement

[1] Red-teaming, in cybersecurity, involves either thinking or acting as the cyber 'attacker' or 'malicious actor', to better understand how organizations and their IT systems should be defended. Penetration testing is, more specifically, a attempt to overcome or evade an organization's cybersecurity measures, usually conducted by an outside contractor, also to identify ways to strengthen that organization's cyber defences.

or intelligence agencies receiving a warrant from a minister or judge. Within the scope of this paper, use of the terms authorized/unauthorized risks reintroducing the confusion regarding legitimacy, described above, between government warrants on the one hand and owner/operator/user permission on the other. The reason the distinction is set out in the paper, and in the principles put forward, in terms of permission rather than authorization is not due to any difference in the intrinsic meaning of the terms; rather it reflects the differing extent to which the two terms are already used in relation to commercial cyber intrusion capabilities.[2]

There are three further aspects of this distinction that need to be set out at this point.

First, permission implies – but does not always include – prior knowledge: the buyer of penetration-testing services knows that the contractor will attempt to infiltrate their networks (permissioned intrusion); but the owner of a device that is compromised by spyware has no idea this is the case (unpermissioned intrusion). However, the user of a device may give permission to all kinds of applications on their device, for a wide variety of reasons, but not be aware of the subsequent behaviour of any one application. Alternatively, user/owner/operator permission may be given for features such as automatic updates in general, which does not equate to knowledge of any specific update – or permission for an update to disrupt usual functions. Permission is therefore not necessarily an indicator of prior knowledge, or any guarantee against malicious or otherwise disruptive behaviour.

The user of a device may give permission to all kinds of applications on their device, for a wide variety of reasons, but not be aware of the subsequent behaviour of any one application.

Second, this paper deliberately excludes *manufacturer* permission from the definition (including only user, owner and operator). In many instances, the inclusion of manufacturer permission would be unnecessary. For example, in high-profile cases discussed later in this paper, the use of mobile spyware without permission of the user/owner/operator was investigated and challenged most robustly by the device manufacturer. However, there is a significant subset of cases where manufacturers work with states to enable access to their users' or customers' systems or devices, whether freely or when compelled to do so.[3] Such 'backdoors', as they are termed, clearly therefore have the permission of the manufacturer, but not of the user, owner or operator.

[2] Similarly, the term 'unpermissioned' – despite its admitted awkwardness – rather than 'permissionless', is deliberately used in this paper. In part, it is intended as a more neutral term, as a means of avoiding any implication that an unpermissioned intrusion is by default 'bad'. In addition, it has been chosen for its novelty: notably, the term 'permissionless' is already in use to describe the difference between centrally controlled and distributed blockchain networks.

[3] In general, this is less common for non-user owners and operators, due to manufacturers' relatively high ability to change the underlying code.

Backdoors are conceptually very similar to cyber intrusion capabilities; indeed, a backdoor identified by anyone but the manufacturer would be a central part of the market discussed below. In addition, even manufacturer-developed backdoors indirectly affect markets for commercial cyber intrusion capabilities, by increasing vulnerabilities and potentially opening access vectors for other actors. However, this paper does not consider manufacturer-developed backdoors further, because of the distinct dynamics – usually based on state obligations – around their creation and maintenance. It does, however, return to the overlaps in governance requirements between cyber intrusion capabilities and other methods of state intelligence collection, including backdoors, in Principle 7.[4]

Third, the aim of the paper is to examine not only the use of cyber intrusion capabilities, but the markets behind those uses. This distinction is also more complex than first appears. Some uses of cyber intrusion capabilities are by actors operating in financially motivated settings, whether unregulated cybercriminal 'black' markets or regulated penetration-testing 'white' markets. In such cases, policy aimed at changing market dynamics also directly changes use: if an actor does not have a financial incentive to conduct a ransomware attack or offer a penetration-testing service, they will not do so.

However, the most controversial uses of cyber intrusion capabilities – by states for intelligence collection – are conducted not for financial motives, but for reasons of law enforcement, national security and espionage. In such cases, market interventions directly affect the incentive structure for actors in the supply chain of such capabilities to their eventual end user, and only indirectly affect the decisions of that end user. Here, any market intervention based on kinds of use (permissioned or unpermissioned, legitimate or illegitimate, etc.) relies on the knowledge, ability and incentive of actors in the supply chain to distinguish between those different kinds of use. This is far from guaranteed: some actors in the supply chain, such as vulnerability researchers, exploit brokers, system integrators and access-as-a-service providers, often claim (rightly or wrongly) not to know the specific purposes their commercially sold capabilities are put to, and rarely have incentives to improve their knowledge or act on it.[5]

Although they affect the decisions of commercial entities, market interventions need to go beyond the level of those entities. As nearly all markets are influenced by state policy and regulation, market interventions should also focus on actions by states – especially in countering what the companion paper in this series calls 'state permissive behaviours' facilitating market growth.[6] This current paper therefore focuses on state interventions regarding commercial cyber intrusion capabilities, considering their multiple roles as users, regulators, investors and detectors.

[4] For similar reasons, this paper does not address the 'passive' collection of target intelligence from a range of commercial entities, other than in Principle 7.
[5] Vulnerability researchers are people who discover and sell knowledge of vulnerabilities in devices and systems. This knowledge can then be used to create 'exploits', which can be bought and sold by exploit brokers, that enable access to those devices and systems via a specific vulnerability. To be most useful, exploits need to be integrated into larger tools by system integrators. At the top end of the integration scale, some companies make 'access-as-a-service' tools that do everything other than select the target.
[6] Mott, G. et al. (2024), *State Permissive Behaviours and Commercial Offensive-Cyber Proliferation*, Occasional Paper, London, RUSI and Royal Institute of International Affairs, https://rusi.org/explore-our-research/publications/occasional-papers/state-permissive-behaviours-and-commercial-offensive-cyber-proliferation. Even black markets are influenced indirectly by states, through their decisions to make certain commodities illegal.

03 Existing interventions

This chapter summarizes policy interventions over the past decade to counter the misuse of commercial cyber intrusion capabilities. These focus variously on governments, companies and individuals, but have been initiated by a relatively narrow group of actors.

The best-known state-based attempt at regulating the market for commercial cyber intrusion capabilities is via the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,[7] which in 2013 added certain capabilities required for 'intrusion software' to its list of dual-use items requiring export controls from signatory states.[8]

The inclusion of intrusion software in the Wassenaar Arrangement has encountered significant obstacles and resistance, both among its members and at the level of state implementation. Much of this resistance has been due to the potential for the Wassenaar Arrangement to unintentionally stifle legitimate security research, which deepened suspicion among cybersecurity communities of export regulation in general.[9]

The US provides the most extreme example of this tension, reflecting both the extensive reach of its domestic export controls, and the lobbying strength of its technology and cybersecurity industry. The US Bureau of Industry and Security (BIS), in the Department of Commerce, approached implementation

[7] For background on the Wassenaar Arrangement, see https://www.wassenaar.org/about-us.
[8] See, for example, Lin, H. and Trachtman, J. (2020), 'Diagonal Export Controls to Counter Diagonal Transnational Attacks on Civil Society', *European Journal of International Law*, 31(3), pp. 917–39, https://doi.org/10.1093/ejil/chaa053; Korzak, E. (2020), 'The Wassenaar experience and its lessons for international regulation of cyber tools', in Tikk, E. and Kerttunen, M. (eds) (2020), *Routledge Handbook of International Cybersecurity*, Abingdon: Routledge, 2020.
[9] Such suspicion stems from repeated government use of export controls to restrict cybersecurity innovations such as cryptography, especially in the US. See Shires, J. (2021), The Politics of Cybersecurity in the Middle East, London: Hurst Publishers.

of the Wassenaar Arrangement's initial addition of intrusion software through a proposed export-control rule, published in 2015. After extensive criticism from the cybersecurity industry, the US not only withdrew this rule, but successfully renegotiated the language of the Wassenaar Arrangement itself with the other participating countries in 2017, leading the US to finally adopt Wassenaar-aligned export controls for intrusion software in 2021.[10]

Elsewhere, the EU incorporated intrusion software export controls into its Dual-Use Regulation in 2021, as one element in a broader list of 'cyber-surveillance' items. Importantly, this regulation includes a 'catch-all' clause (Article 5.1–2), allowing for the control of items beyond those listed if EU states or exporters believe those items are intended for use 'in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law'.[11]

In addition to Wassenaar, over the last two years there have been many new initiatives to counter the misuse of commercial cyber intrusion capabilities, including:

- The EU Parliament's PEGA Committee, formed in 2022 to investigate the use of the Israeli NSO Group's Pegasus spyware by EU states and other countries in contravention of EU law, especially human rights law. The PEGA committee published its findings in 2023.[12]
- US unilateral measures on companies and individuals involved in commercial cyber intrusion markets. These measures began with the imposition of export controls for US technologies, products and services to NSO Group and three other companies in 2021,[13] and continued with an executive order preventing US government use of certain kinds of spyware in 2023.[14] The most recent action by the US at the time of writing was financial sanctions on another consortium, Intellexa, in 2024.[15] Also in 2024, the US introduced a new policy

[10] See, for example, Hinck, G. (2018), 'Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research', Lawfare, 5 January 2018, https://www.lawfaremedia.org/article/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research; U. S. Department of Commerce, Bureau of Industry and Security (2021), 'Information Security Controls: Cybersecurity Items', *Federal Register*, 21 October 2021, https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items.

[11] European Union (2021), '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)', https://eur-lex.europa.eu/eli/reg/2021/821/oj.

[12] Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (2023), *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*, European Parliament, 8 May 2023, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf. See also Richard, L. and Rigaud, S. (2023), *Pegasus: The Story of the World's Most Dangerous Spyware*, London: Macmillan.

[13] U.S. Department of Commerce (2021), 'Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities', press release, 3 November 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[14] The White House (2023), 'Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security', 27 March 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.

[15] U.S. Department of the Treasury (2024), 'Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium', press release, 5 March 2024, https://home.treasury.gov/news/press-releases/jy2155. For an extended investigation, see Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024), 'Markets Matter: A Glance into the Spyware Industry', Digital Forensic Research Lab, 22 April 2024, https://dfrlab.org/2024/04/22/markets-matter-a-glance-into-the-spyware-industry.

allowing visa restrictions on individuals involved in spyware misuse.[16] It has several other proposed bills in motion.[17]

- A joint statement on spyware adopted by 11 states at the US-hosted Summit for Democracy in 2023, committing to various measures to restrict the commercial market for cyber intrusion capabilities.[18] These measures include strengthening internal human rights protections, more rigorous export controls, information-sharing and international coalition-building. The statement was updated at the 2024 summit, after six more states joined the commitment; and again in September, on the margins of the UN General Assembly, when four further states endorsed the statement.[19]
- An Export Controls and Human Rights Initiative (ECHRI) code of conduct, released at the 2023 Summit for Democracy by the US and 24 other states.[20] The code of conduct, originally proposed at the inaugural summit in 2021,[21] lists voluntary actions to apply export controls to prevent the misuse of 'surveillance tools', whether or not states participate in other export-control groups like the Wassenaar Arrangement.
- A 'blueprint' on 'taming the cyber mercenary market', released in 2023 by the Paris Peace Forum, as part of its Call for Trust and Peace in Cyberspace. The blueprint is the result of a long-standing working group within the Peace Forum on cyber mercenaries, and includes both a restatement of the reasons for intervention and several specific suggestions for action.[22]
- Industry principles to curb cyber mercenaries, put forward by the Cyber Tech Accord (CTA) in 2023.[23] While these principles overlap in several areas with those set out in this paper – suggesting that the overall scope for intervention is not that wide – there is a crucial difference in that the CTA principles are focused solely on industry action, given that the CTA is an agreement between companies rather than governments.

[16] U.S. Department of State, 'Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware', press statement, https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware. The first use of this policy was in April 2024, with 13 individuals listed: see U.S. Department of State (2024), 'Promoting Accountability for the Misuse of Commercial Spyware', press statement, 22 April 2024, https://www.state.gov/promoting-accountability-for-the-misuse-of-commercial-spyware.

[17] Notably, H.R.5440 - Protecting Americans from Foreign Commercial Spyware Act (https://www.congress.gov/bill/118th-congress/house-bill/5440) and H.R.5522 - Combatting Foreign Surveillance Spyware Sanctions Act (https://www.congress.gov/bill/118th-congress/house-bill/5522/text) were introduced in the House of Representatives in September 2023.

[18] Administration of Joseph R. Biden, Jr (2023), 'Joint Statement on Efforts To Counter the Proliferation and Misuse of Commercial Spyware', Office of the Federal Register, National Archives and Records Administration, 30 March 2023, https://www.govinfo.gov/app/details/DCPD-202300249.

[19] As at September 2024, the 21 signatories are Australia, Austria, Canada, Costa Rica, Denmark, Estonia, Finland, France, Germany, Ireland, Japan, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Sweden, Switzerland, the UK and the US. See U. S. Department of State (2024), 'Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware', media note, 22 September 2024, https://www.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware.

[20] U.S. Department of State (2023), 'Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy', media note, 30 March 2023, https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy.

[21] The White House (2021), 'Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy', 10 December 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy.

[22] Paris Peace Forum (2023), 'Paris Call: Taming the Cyber Mercenary Market', 10 November 2023, https://parispeaceforum.org/publications/paris-call-taming-the-cyber-mercenary-market.

[23] Cybersecurity Tech Accord (2023), 'New industry principles to curb cyber mercenaries', 27 March 2023, https://cybertechaccord.org/new-industry-principles-to-curb-cyber-mercenaries.

- The Pall Mall Process, a multi-stakeholder initiative launched by the UK and French governments in 2024, including a declaration with four pillars of accountability, precision, oversight and transparency.[24]

These initiatives range from high-level, abstract goals to very concrete steps against specific individuals or companies. The specific actions taken are summarized in Table 1. This table is not intended to be a complete list of all interventions, but a smaller selection based on their profile in public discourse and their specificity. The information given in the table summarizes highly complex policies in ways that necessarily omit some important details, so the original sources should be referred to for the full intervention. Table 1 also points to a clear geographic bias. The most international intervention is the Wassenaar Arrangement, established in the mid-1990s as the successor to the Cold War-era Coordinating Committee on Multilateral Export Controls (COCOM); it currently has 42 participating states.[25] More recent interventions predominantly come from the US, Europe or their close allies. The Pall Mall Process has a deliberately wider scope, incorporating many countries outside the Wassenaar Arrangement, including in the Global South.

Table 1. Selected interventions in the ecosystem for commercial cyber intrusion capabilities, 2013–24

Initiative	Focus	Type of action	Reason for action
Wassenaar Arrangement amendment (2013) https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2813%29%201.pdf, p. 209	Governments	Require export controls from governments	Prevent human rights violations; reduce risks to national security
US entity list (NSO and others) (2021) https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list	Companies	Impose export controls on named companies	Prevent transnational repression; protect privacy and security
Export Controls and Human Rights Initiative (ECHRI) code of conduct (2021–23) https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy	Governments	Update export controls	Prevent human rights violations; protect privacy; address risks to international security
Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware (2023–24) https://www.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware	Governments	Create guardrails for government use	Prevent human rights violations; uphold rule of law; protect civil rights and civil liberties

[24] Foreign, Commonwealth & Development Office (2024), 'The Pall Mall Process declaration: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities', 6 February 2024, https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities. See also Herpig, S. and Paulus, A. (2024), 'The Pall Mall Process on Cyber Intrusion Capabilities', Lawfare, 19 March 2024, https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities; Baram, G. (2024), 'The Pall Mall Process could be a catalyst for international collaboration on commercial cyber intrusion capabilities', Binding Hook, 25 March 2024, https://bindinghook.com/articles-hooked-on-trends/the-pall-mall-process-could-be-a-catalyst-for-international-collaboration-on-commercial-cyber-intrusion-capabilities.

[25] The current membership is: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, South Korea, Romania, Russia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, the UK and the US. India is the most recent country to join, in 2017.

Initiative	Focus	Type of action	Reason for action
Joint Statement (2023–24)	Governments	Require export controls from governments	Prevent malicious use
Paris Call for Trust and Security in Cyberspace (2023) https://parispeaceforum.org/publications/paris-call-taming-the-cyber-mercenary-market	Governments	Create guidelines for acceptable use	Comply with domestic law and international obligations
Paris Call (2023)	Governments	Develop transparent procurement processes and vendor verification	Comply with UN Guiding Principles on Business and Human Rights; prevent human rights abuse
Paris Call (2023)	Governments	Require export controls from governments	Prevent malicious use and use by non-state actors
Paris Call (2023)	Governments	Develop company blacklists, restrict market access	Prevent violations of international norms and human rights
Paris Call (2023)	Companies	Conduct investor due diligence	Prevent human rights violations
Paris Call (2023)	Individuals	Create guardrails for former government individuals	Prevent misuse and abuse
PEGA Committee (2023) https://www.europarl.europa.eu/committees/en/pega/documents/latest-documents	Governments	Remove EU funding from spyware research	Prevent human rights violations; prevent spyware abuses under 'national security' guise
PEGA Committee (2023)	Governments	Regulate vulnerability discovery process at EU level	Prevent human rights violations; prevent spyware abuses under 'national security' guise
US H.R.5440 (bill introduced 2023) https://www.congress.gov/bill/118th-congress/house-bill/5440	Governments	Impose restrictions on foreign assistance	Prevent targeting of US citizens (some consideration of citizens of other countries)
US H.R.5522 (bill introduced 2023) https://www.congress.gov/bill/118th-congress/house-bill/5522	Individuals	Impose financial sanctions on individuals involved	Reduce risks to national security; prevent targeting of US citizens; prevent human rights violations and repression
Pall Mall Process (2024) https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities	Governments	Norm of accountability	Comply with international human rights law
Pall Mall Process (2024)	Governments	Norm of precision	Prevent unintended, illegal or irresponsible consequences of use
US Intellexa sanctions (2024) https://home.treasury.gov/news/press-releases/jy2155	Companies	Impose financial sanctions on named companies	Prevent targeting of US citizens; prevent human rights violations and repression
US visa restrictions (2024) https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware	Individuals	Visa restrictions on individuals and families involved in or benefiting from misuse	Prevent misuse

As illustrated in Table 1, these interventions seek to variously focus on governments, companies and individuals. The type of action also varies, with some interventions seeking to affect government behaviours (as with Wassenaar export controls, which require governments to alter and implement export-control measures, even though those measures ultimately affect companies), or the less structured guardrails or guidelines for government use under the Paris Call and Pall Mall Process. Other interventions direct government action against companies (US sanctions), or company action against other companies (such as the Paris Call's suggestion for investor due diligence).

These interventions are also explicitly conducted for a wide variety of reasons, ranging from unspecified misuse, abuse and malicious activity to more specific violations of international law or human rights, or even targeting of a state's citizens (in the case of the US). Many of the justifications for intervention link commercial cyber intrusion capabilities to transnational repression, instability and insecurity in cyberspace, or lack of compliance with norms of responsible state behaviour established at the UN.

04 Scope and limitations

Markets for commercial cyber intrusion capabilities are large and diverse, with different approaches required for different areas and problems. But existing interventions are unlikely to encourage substantive change across the whole landscape.

The overview of interventions given in the previous chapter shows how civil society, industry and state actors have proposed a wide range of policy interventions in recent years. This is a good start: markets for commercial cyber intrusion capabilities are large and diverse, with different approaches required for different areas and problems within this space. However, the multiple interventions that so far exist are unlikely to encourage substantive change across the whole landscape. To achieve such substantive change, this paper recommends a set of principles for state approaches to *all* markets for commercial cyber intrusion capabilities. It does so for two reasons:

First, more concrete actions, such as sanctions or export controls, are likely be attractive only to those states with the power to affect global markets unilaterally, such as the US, or to those with already high capacity and favourable contexts for regulation, such as the EU. Even then, the sheer range of actions summarized in Chapter 3 risks incoherence and inconsistency within this relatively like-minded group. In this context, a set of principles can help to link the interventions described to create a coherent package that can achieve consensus from multiple perspectives, from narrow national security objectives to broader concerns regarding human rights or the security of the internet architecture.

Second, many high-profile states accused of misusing commercial cyber intrusion capabilities are not party to the policies and commitments described, and in some cases are the direct target of the actions listed in the previous chapter – for example, to prevent a geopolitical competitor from gaining access to commercial cyber intrusion capabilities. There is a real possibility of a schism between two markets: a highly regulated, predominantly Western market with potentially lower profit margins, characterized by established internal trust and transparency mechanisms between allies; and a broader global market with higher profit margins and far less – or no – regulation. A set of principles can help to identify areas of common interest between these two sets of states, where there are opportunities for high-level agreement on aims even if certain countries disagree on specific ways to achieve those aims, or on the interpretation and treatment of specific cases.

There are, nonetheless, limits to the scope of change envisioned by the principles. Influential observers, such as UN special rapporteurs, have called for a moratorium or ban on some kinds of commercial cyber intrusion capabilities altogether – especially spyware – due to their 'life-threatening' impact on privacy, individual security and human rights.[26] However, such a proposal may not be achievable: the demand for commercial cyber intrusion capabilities, primarily from states looking to expand their cyber military or intelligence capabilities, is probably too powerful. This paper assumes that states and other actors will continue to acquire and use commercial cyber intrusion capabilities in the short and medium term.

Influential observers, such as UN special rapporteurs, have called for a moratorium or ban on some kinds of commercial cyber intrusion capabilities altogether – especially spyware – due to their 'life-threatening' impact on privacy, individual security and human rights.

Conversely, potential changes in the technological environment could limit the relevance of commercial cyber intrusion capabilities. Software development could become significantly more secure, with prevalent vulnerability classes removed,[27] or trends towards device compromise could be supplanted or replaced by system- or network-wide capabilities.[28] This would be a reversal of the current trend, where the proliferation of cyber intrusion capabilities is in part a response to greater encryption adoption after major scandals relating to global intelligence collection, such as the Snowden revelations. Nonetheless, the paper assumes that, in the short and medium term, market incentives for insecure software will continue to generate the supply of, as well as demand for, commercial cyber intrusion capabilities.

[26] Office of the High Commissioner for Human Rights (2021), 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech', press release,12 August 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.
[27] A recent leak from the cyber-forensics company Cellebrite shows a significant lag in (physical) access to recent iPhone models, supporting this hypothesis. See Cox, J. (2024), 'What Phones Cellebrite Can (and Can't) Unlock', 404 Media, 17 June 2024, https://www.404media.co/leaked-docs-show-what-phones-cellebrite-can-and-cant-unlock.
[28] See, for example, Shwartz, M. (2024), 'The boom, the bust, the adjust and the unknown', presentation at Zer0con 2024, April 2024, https://www.slideshare.net/slideshow/zer0con-2024-final-share-short-versionpdf/267171223.

05 Workshop discussions

The cyber policy team at Chatham House convened a workshop at which expert stakeholders from multiple disciplines discussed responsible approaches to commercial cyber proliferation. This chapter provides a summary of the discussions, including participants' reactions to earlier versions of the principles presented in this paper.

On 22 March 2024, the Chatham House International Security Programme's cyber policy team hosted a workshop on understanding and investigating responsible activity in commercial cyber proliferation. The workshop brought together stakeholders from multiple disciplines, including companies developing and using cyber intrusion capabilities, multinational technology companies, civil society representatives and relevant UK government entities. The research team presented an overview of existing interventions, as well as earlier versions of the principles set out in this research paper.

This chapter provides a summary of ideas and perspectives shared during the workshop discussion, including participants' reactions to the draft principles. Specific comments from individual participants are quoted where relevant. As the workshop was held under the Chatham House Rule,[29] no participant or organization represented is identified.

[29] When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Three main themes emerged from the workshop:

- **The need for a holistic approach to governance and regulation of commercial cyber intrusion capabilities**, taking into account the interconnections between markets as well as their distinct characteristics, and recognizing that different states take substantially different views of a market's benefits and risks.
- **The importance of individual moral decisions in preventing misuse**, recognizing that individuals operate within commercial and political structures that limit the impact of such decisions, and that resorting to 'ethics' can be an excuse rather than a policy.
- **The global nature of the issue**, meaning that regional efforts to regulate markets are likely to be only partially effective, and that even effective policies in one region may have unintended and diametrically opposed consequences in another.

Regarding the first theme, workshop participants emphasized the restrictions on scope discussed in the previous chapter. Some argued that policymakers 'should look at the liability of software publishers'; as one participant put it: 'If [technology companies] had software quality, [industry] wouldn't have these problems.' Others highlighted what they perceived to be an inevitability about the market, summarized by one participant as: 'There's always going to be some level of activity – it's not an all or nothing situation.' In contrast, however, one participant noted that 'penetration testing has too much weight behind it' as a component of cybersecurity, thereby implying that many industry players overstate the importance of permissioned intrusion to cyber defence. Some participants voiced concern regarding the different incentives for engaging in market restriction. As one put it: 'Russia and China do not care about individuals – you have to show them the impact on national security.' The irony was also highlighted that the 'Western' response to market problems is to introduce more bureaucracy (technical as well as organizational), while adversaries reduce theirs.

During the workshop, the research team clarified that 'unpermissioned' is not a synonym for 'illegal' or 'undesirable': rather, unpermissioned intrusion should trigger additional safeguards and thresholds.

Participants generally agreed with the project's focus on state behaviours, with one suggesting: 'The mission of a company is to sell things – there are rules, and the rest is the responsibility of the state.' Another said: 'We need to start with governments … they should be held accountable.' However, some were sceptical regarding the potential for changing such behaviours, as well as about the robustness of any regulatory approach that was not global in scope, asking: 'Do you not want to have a capability because you made a decision not to engage with that country? … Is there no access juicy enough that a friendly state wouldn't bend their rules?'

Regarding the second theme, participants engaged in lengthy discussion about the relevance of and potential for individual ethics. Some argued that 'self-governance' is already prevalent, while others were more sceptical. Participants also challenged the distinction between permissioned and unpermissioned intrusion along ethical lines, instinctively categorizing responsible state cyber operations as fundamentally different to state abuse of commercial cyber intrusion capabilities. As one participant put it: 'You're either breaking the law or you're not.'

During the workshop, the research team clarified that 'unpermissioned' is not a synonym for 'illegal' or 'undesirable': rather, unpermissioned intrusion should trigger additional safeguards and thresholds. Despite the inevitable crudeness of any binary distinction in this complex area, this paper introduces the distinction between permissioned and unpermissioned intrusion to prevent exactly this line of thought – i.e. that 'responsible' cyber operations are not a key part of the overall problem set.[30] Instead, the paper sees *all* unpermissioned activity as requiring greater regulatory and industry scrutiny.

The third general theme highlighted by the workshop discussion concerned the scale of the market globally, in terms of companies and individuals. Some participants expressed the view that the number of people at the centre of supply chains for high-end commercial cyber intrusion capabilities is relatively small – in the hundreds, not thousands. They therefore considered that interventions should – like the US visa restrictions noted above – seek to change the incentive structure for this small pool. Other participants, however, highlighted the potential for the existing pool to grow, commenting that the 'talent pool is truly global', and 'a lower-tier hacker is three months of study away from being a higher-tier hacker'. Consequently, participants identified that there is 'some risk of governments overcompensating in controlling the market, pushing [individuals] to other states who are willing to pay'.

The workshop provided an important testing ground for the approach taken by the research project, with welcome challenges and creative ideas to further refine the work on this paper. Many of the ideas and themes discussed at the workshop are incorporated in the principles put forward in the next chapter.

[30] National Cyber Force (2023), *Responsible Cyber Power in Practice*, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice.

06 Principles for state approaches

This chapter presents eight principles for state approaches to commercial cyber intrusion capabilities, and draws further on observations offered by participants at the expert stakeholder workshop.

The principles for state approaches to commercial cyber intrusion capabilities are set out in five thematic sections (A–E). The principles themselves are interlinked, with each principle being logically necessary to establish the later principles. In line with the high-level approach of this paper, the discussion in this chapter provides only examples of specific actions that might fall under these principles, rather than detailing the implementation of each principle. In addition, there are many cases that pose conceptual or practical challenges to certain principles. Such cases are discussed where relevant in this chapter – often drawing further on comments from participants at the workshop summarized in Chapter 5 – especially because they help to sharpen the overall purpose of the principles and to clarify conceptual boundaries. Due to the complexity of such cases, their interpretation given here is not definitive; others may take different views.

A. Increasing internal coherence

Principle 1: States should align their approaches across markets for commercial cyber intrusion capabilities, including as customers and users, investors, detectors and defenders, and regulators.

Different state entities are likely to be responsible for these various roles. Importantly, however, states should work to prevent contradictions between their policies and actions in all of these areas: for example, they should take clear steps to avoid investment by one state body in a commercial cyber intrusion company that is subject to investigation or sanction by another entity of the same state. In some cases, there may be good reasons to maintain adversarial relationships between state entities – for instance, where a law enforcement agency seeks to use commercial cyber intrusion capabilities for legitimate criminal investigations, while a national cybersecurity centre seeks to detect and neutralize such capabilities. In such cases, states should ensure that there is an independent oversight mechanism to reconcile these different purposes.

One example of alignment is a vulnerabilities equities process (VEP), which governs state decisions to retain vulnerabilities for exploitation (unpermissioned use) or release them for patching.[31] However, as participants in the workshop summarized in Chapter 5 emphasized, VEPs are not a straight choice between permissioned and unpermissioned uses. While the main purpose of release is patching, release will also lead to permissioned uses (as penetration testing companies incorporate that vulnerability into their services), as well as unpermissioned uses by actors other than the state involved (including cybercriminals as well as other states). In the case of the UK, therefore, its assertion that the 'starting position [of a VEP] is always that disclosing a vulnerability will be in the national interest'[32] encapsulates a wide range of risks in an effort to align several – sometimes competing – state interests.

One example of alignment is a vulnerabilities equities process (VEP), which governs state decisions to retain vulnerabilities for exploitation (unpermissioned use) or release them for patching.

While the example of VEPs focuses on tactical alignment by addressing individual vulnerabilities on a case-by-case basis, states can also align different roles at the strategic level (for example, in state cybersecurity, data protection and computer misuse legislation). An example of misalignment at this level would be computer misuse legislation that criminalizes or fails to provide sufficient exemptions for 'good faith' cybersecurity research, while state cybersecurity strategies or data protection legislation recommend and support such research. Another example is when different state agencies independently procure identical capabilities from the same vendor, potentially increasing prices and resulting in inconsistent contractual obligations regarding use thresholds and abuse procedures.[33]

Misalignment can be either unintentional or deliberate, resulting from divergent goals within different state bodies. In the former case, increasing internal coherence is a relatively straightforward matter of improving information flows and understanding of other positions. In the case of deliberate misalignment, increasing coherence requires far more substantial policy choices and political negotiation.

[31] For more detail, see Fidler, M. (2024), 'Zero Progress on Zero Days: How the Last Ten Years Created the Modern Spyware Market', Neb. L. Rev., 102(713), https://ssrn.com/abstract=4626426.
[32] Government Communications Headquarters (GCHQ), 'The Equities Process', https://www.gchq.gov.uk/information/equities-process.
[33] Shires (2021), *The Politics of Cybersecurity in the Middle East*.

B. Supporting permissioned intrusion

Principle 2: States should separate markets for permissioned cyber intrusion from markets for unpermissioned cyber intrusion as far as possible: administratively, legally and technologically.

One source of complexity in the ecosystem for commercial cyber intrusion capabilities is an extensive overlap between markets for permissioned and unpermissioned intrusion. This overlap exists at the vulnerability discovery stage, where vulnerability researchers can sell a vulnerability to actors for permissioned or unpermissioned intrusion, or to actors where the researcher does not know what it will be used for.[34] Indeed, economic incentives and market opacity encourage researchers to sell single vulnerabilities multiple times, often for different uses.

This overlap narrows as vulnerabilities are developed into sophisticated intrusion services. Workshop participants suggested that the resource investment needed to provide a proof-of-concept exploit for a bug bounty is much lower than that required to integrate that exploit into malware.[35] As one participant put it: 'No-one sells a proof of concept to a law enforcement agency.' Similarly, no penetration testing service needs to use (or pay for) a whole spyware architecture, although it might make use of the same vulnerabilities.[36] For less sophisticated and bespoke tools, however, the technological overlap is almost complete. A malware framework used for penetration testing could be exactly the same as one used for unpermissioned intrusion. And, of course, permissioned and unpermissioned intrusion also rely heavily on the same open-source tools.[37]

Workshop participants emphasized these overlaps, with one noting: 'You can't separate [the two markets] at point of sale; it has to be at point of use.' Others were even sceptical of any useful distinction at point of use. As one put it: 'Would the customer really tell you what they would use it [i.e. the exploit] for?' Despite these technological overlaps and challenges regarding user trust, participants recognized the possibility for a 'legal and policy framework to help separate the market', as 'imposing separation between different activities isn't new' from an organizational perspective – as in banking or auditing, for instance. A further example from the financial services sector is the separation in banking activities between investment and customer banking: after the 2008 financial crash, banks in some countries were forced to administratively separate activities that had previously been tightly connected.

[34] Or even, in some reported cases, buyers intending one use masquerade as the other, fraudulently claiming to have permission for a particular intrusion.
[35] A bug bounty is a programme in which a company offers a financial reward for the discovery of vulnerabilities ('bugs') in its systems. Most bug bounty programmes operate through platforms that connect companies and vulnerability researchers, such as BugCrowd or HackerOne.
[36] See, for example, Dowd, M. (2023), 'Inside the Zero Day Market', presentation at BlueHat, October 2023, https://nocomplexity.com/wp-content/uploads/2024/06/bluehat2023-mdowd-final.pdf.
[37] See, for example, Naraine, R. (2022), 'Proofpoint: Watch Out for Nighthawk Hacking Tool Abuse', SecurityWeek, 23 November 2022, https://www.securityweek.com/proofpoint-watch-out-nighthawk-hacking-tool-abuse. For malware frameworks, the classic example is Cobalt Strike, most recently (at the time of writing) the subject of a law enforcement operation in mid-2024: see Lakshmanan, R. (2024), 'Global Police Operation Shuts Down 600 Cybercrime Servers Linked to Cobalt Strike', The Hacker News, 4 July 2024, https://thehackernews.com/2024/07/global-police-operation-shuts-down-600.html.

Other workshop participants pointed to successful examples of technological use conditions, such as watermarking certain exploits to trace particular end users, thereby 'incentivizing the end user to be more responsible' and 'removing that blanket of deniability'. In one case discussed by participants, a watermark was applied to an exploit sold to a law enforcement agency, helping the seller identify that exploit if it was later transferred to other actors. However, the length of supply chains for cyber intrusion capabilities was a repeated concern, with resellers, distributors, brokers and system integrators all acting as intermediaries who would each need to verify from their customer the intended use of a particular tool.

Given such overlaps, states should look to create administrative and legal separation between government entities that are engaged in permissioned and unpermissioned cyber intrusion. Where the same government entity conducts both, states should introduce administrative separation within that entity, and also look to enforce a similar administrative separation for their commercial providers. For example, the same separation should be required of a defence contractor that develops tools for unpermissioned intrusion and also offers a commercial penetration testing service.

Separation should also apply to government entities that operate within the supply chain for cyber intrusion capabilities, such as vulnerability research. At one end of the spectrum, the UK government took extensive steps to ensure that its Huawei Cyber Security Evaluation Centre (HCSEC) would not be perceived as identifying vulnerabilities for exploitation rather than for security, demonstrating extensive separation.[38] At the other, some reports have suggested that China's new vulnerability disclosure law and independent hacker ecosystem offer opportunities for state unpermissioned intrusion, indicating very low levels of separation.[39] Leaked data from Chinese cybersecurity company Isoon in February 2024 suggest that this company developed an 'automated penetration testing platform' to conduct unpermissioned intrusion for Chinese intelligence agencies,[40] as well as pointing to discussions about the Chinese government obtaining zero-days (i.e. vulnerabilities unknown to the manufacturer and therefore without an available patch) from a public hacking competition.[41]

From a more commercial perspective, the public-facing presentation of zero-day research brokers deliberately blurs the lines between cybersecurity research (permissioned) and government use of zero-day exploits (unpermissioned). While such organizations argue that this blurring is, as one puts it, 'the only way to support the zero-day research community',[42] this is not a natural or inevitable

[38] BBC News (2020), 'Huawei 'failed to improve UK security standards', 1 October 2020, https://www.bbc.co.uk/news/technology-54370574.

[39] Greenberg, A. (2023), 'How China Demands Tech Firms Reveal Hackable Flaws in Their Products', *Wired*, 6 September 2023, https://www.wired.com/story/china-vulnerability-disclosure-law; Benincasa, E. (2024), *From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem*, Zurich: Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/f/r/o/m/from_vegas_to_chengdu_hacking_contests_b.

[40] BushidoToken (2024), 'Lessons from the iSOON Leaks', 22 February 2024, https://blog.bushidotoken.net/2024/02/lessons-from-isoon-leaks.html.

[41] KELA Cyber Intelligence Center (2024), 'I-Soon leak: KELA's insights', 7 March 2024, https://www.kelacyber.com/i-soon-leak-kelas-insights.

[42] Zerodium (undated), 'Frequently Asked Questions | About Zerodium | What is Zerodium', https://zerodium.com/faq.html.

outcome; rather, it is the outcome of market incentives shaped by states as users, buyers and regulators. State actions, then, can shift market incentives to make the separation recommended here commercially viable for companies on both sides.

States should also ensure that companies offering tools for permissioned cyber intrusion make best efforts – including via customer relations, due diligence and access control – to prevent use of these same tools for unpermissioned intrusion. Workshop participants offered some creative ideas in this regard, such as deciding on likelihood of permissioned or unpermissioned intrusion based on the type of contract in question. It was suggested that if a contract's terms included payment or licence per successful intrusion, it was far more likely to be for unpermissioned use than permissioned. If such contractual or other bureaucratic characteristics could be reliably and efficiently assessed by states, they could be used to determine whether a particular sale should be governed by separate regulatory regimes for permissioned and unpermissioned uses.

Importantly, this principle is not intended as an immediate clean break between markets for permissioned and unpermissioned cyber intrusion. It is recognized that the current level of entanglement means a wholly clean break is likely to be impractical for most if not all states. Instead, as the examples above suggest, there are multiple steps states could take to move further away from highly overlapping markets (the current situation) to much lower levels of overlap, or at least to halt the movement towards less separation exemplified by China's vulnerability disclosure law and opaque zero-day brokers.

States should ensure that companies offering tools for permissioned cyber intrusion make best efforts – including via customer relations, due diligence and access control – to prevent use of these same tools for unpermissioned intrusion.

As indicated at the start of this chapter, this principle is dependent on the first – i.e. achieving, as far as possible, internal coherence. Separating the administrative and regulatory architecture around markets oriented towards permissioned and unpermissioned intrusion is only helpful if a state can coordinate effectively between them.

Principle 3: States should stimulate markets for permissioned use of commercial cyber intrusion capabilities.

Given that Principle 2 provides for increasing separation between markets for permissioned and unpermissioned cyber intrusion capabilities, this principle envisages that states should stimulate the former. Principle 3 also presumes some level of consistency in oversight and coherence across state capacities, as put forward in Principle 1.

Importantly, because different state entities are primary actors within markets for permissioned and unpermissioned cyber intrusion capabilities, stimulating one market does not necessarily imply prioritization of that market over the other. As already stated, the goal is not to remove the market for unpermissioned intrusion entirely; rather, the aim is to place it in a different regulatory environment from the wider market for permissioned intrusion.

That said, the discussion by workshop participants, summarized in Chapter 5, on the so-far limited size of the talent pool suggests that combining stimulation and separation (Principles 2 and 3) could – and should – lead individuals to move from unpermissioned markets towards permissioned ones. This could be encouraged by increasing incentives (financial, motivational and community) for vulnerability researchers and companies to sell for permissioned uses. If separation would create financial pressures on individuals and companies operating across both markets, then stimulation is intended to alleviate those pressures. As such, both principles are intended to work in tandem.

Some workshop participants questioned the feasibility of the combined principles of separation and stimulation by giving examples of companies that only sell to Five Eyes states (Australia, Canada, New Zealand, the UK and the US) – 'so they can sleep at night', as one put it – while also highlighting the financial incentives against such restrictions, mainly 'the buying power of countries outside the Five Eyes that make it difficult to resist'. However, it is not clear that such companies already participate extensively in markets for permissioned intrusion, and so the principles of separation and stimulation do not significantly change their incentive structure. As stated above, this principle does not prevent states from investing in markets for unpermissioned intrusion (whether individually or within security alliances), but instead suggests they should – at least equally – stimulate markets for permissioned intrusion.

States can use multiple levers to stimulate markets for permissioned intrusion. At the broadest level, states could build capacity from the ground up through educational initiatives to explain the significance of permissioned intrusion, and differences from unpermissioned intrusion. This education could be made available to school or university students as well as via relevant professional courses. Accredited state schemes for permissioned intrusion can also stimulate and regulate these markets.

More directly, states could use government procurement processes to support permissioned intrusion, enhancing separation by favouring contractors with strict organizational and technological constraints on preventing unpermissioned use. Equally effective levers could be found at the individual level, such as recognition or certification programmes for cybersecurity professionals and companies engaged in permissioned intrusion, along the lines of existing ethical hacking certifications.[43] States could also influence the career direction of personnel who leave government service, through financial or more value- and culture-based incentives. The aim would be to encourage outgoing or former employees

[43] Several organizations offer training in 'ethical hacking', with the term usually referring to what this paper calls permissioned intrusion. One of the most well-known is EC-Council's Certified Ethical Hacker (CEH) qualification: see https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh.

into permissioned markets even when their work within state structures has focused on conducting unpermissioned intrusion, rather than moving to work on unpermissioned intrusion commercially.

C. Limiting end users for unpermissioned intrusion

Principle 4: States should not engage commercial actors to independently conduct unpermissioned cyber intrusion on their behalf.

This principle seeks to prevent all commercial actors from independently conducting unpermissioned cyber intrusion on behalf of states. A range of state actions could take place under this principle, including naming and shaming both commercial actors using such capabilities and their suppliers, as well as applying financial sanctions or export-control conditions. Importantly, this principle addresses only commercial actors involved in unpermissioned cyber intrusion *on behalf of* states; its purpose is not to tackle the wider issue of non-state actors engaging in unpermissioned cyber intrusion in other situations.

The other crucial word is *independently*. This principle does not seek to exclude commercial actors from the supply chain for state capabilities for unpermissioned cyber intrusion. Neither does it seek to prevent commercial actors from providing 'turnkey' or 'access as a service' products, such as spyware, to states. In such cases, states remain the end user of such capabilities, and intrusion is not conducted independently. In contrast, independently conducting cyber intrusion gives the commercial actor far more decision-making power in terms of how and when to conduct the intrusion – for example, if a state provides only a list of target names, devices, or even more general tasking instructions. This granular definition of independence contrasts with an alternative commonly dubbed 'finger on the trigger', which implies a relatively straightforward analogy with kinetic weapons. For cyber capabilities, the reality is a more nuanced spectrum of contributions, from provision of a user interface for 'point and click' intrusion at one end (*not* independent conduct, even if a commercial actor helps to train and troubleshoot state users of that interface) to full operational discretion at the other (independent conduct).

A key area of ambiguity lies in military cyber operations. In conventional spheres of military operation, national laws and international agreements (especially the Montreux Document, concerning the operations of private military and security companies during armed conflict) govern the role commercial actors can play in military operations.[44] In line with the research that has informed this paper, it is suggested that if the relationship between states and commercial cyber intrusion companies meets standards for private military contractors set out in the Montreux Document Part 1A (Contracting States), then such companies can be excepted from

[44] For fuller details of the Montreux Document, including the full text of the document, see Montreux Document Forum (2024), 'The Montreux Document on private military and security companies', https://www.montreuxdocument.org/about/montreux-document.html.

the scope of this principle. Exempted companies should then be permitted to act on states' behalf and treated equivalently to private military contractors, with the same standards and obligations.

Going beyond the Montreux Document, states should look to place commercial actors as far from the 'front line' of cyber operations as possible. Unlawful and unpermissioned cyber intrusion by non-exempted companies or other non-state actors (such as hacktivist organizations or unstructured 'IT armies') should still be prohibited.[45] In the absence of a similar international mechanism, law enforcement and other national security applications of unpermissioned cyber intrusion capabilities should be reserved for state actors.

Because commercial intermediaries sell to other commercial entities before ultimate use by a state, a necessary precursor to implementation of Principle 4 would then be 'know your customer' requirements, for intermediaries to ensure sellers are aware of their ultimate recipient.

This principle was the subject of intense discussion in the workshop summarized in Chapter 5. One participant said plainly: 'Some states won't want to sign up to this principle because they like having [the] ability to give these tools [for unpermissioned intrusion] to non-state actors.' Others questioned the distinction between private and public actors in this space, with one asking: 'How much of a contractor do you have to be before becoming a state actor?' This is a lively research area in cyber conflict studies, with scholars differing on the definition and appropriate response – legally and practically – to state 'proxies'.[46] Some workshop participants raised questions around specific countries. One asserted that 'hacker for hire' companies are engaged with no transparency, going as far as to say that some states are also 'silencing reporting on this'.[47] Some participants suggested that some of 'the West's' adversaries have different appetites for contractors to work independently from state direction. However, others pointed out that in times of crisis (the example given was the war in Ukraine) 'Western' states and their allies might also wish to retain the option of co-opting or directing non-state actors.[48]

Ultimately, the implementation of this principle raises many of the same issues as those noted in the discussion of Principle 2 with regard to transparency and knowledge in commercial transactions. Because commercial intermediaries sell to other commercial entities before ultimate use by a state, a necessary precursor

[45] Vignati, M. (2023), 'Civilian hackers blur the lines of modern conflict', Binding Hook, 13 December 2023, https://bindinghook.com/articles-hooked-on-trends/civilian-hackers-blur-the-lines-of-modern-conflict.
[46] Maurer, T. (2018), *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge: Cambridge University Press.
[47] For a published article on the example obliquely referred to by the workshop participant, see Schaffer, M. (2024), 'How a Judge in India Prevented Americans From Seeing a Blockbuster Report', Politico, 19 January 2024, https://www.politico.com/news/magazine/2024/01/19/india-judge-reuters-story-00136339.
[48] I thank an anonymous review for also making this point – and for highlighting the wider questions of escalation and international law that this raises. See also Vignati (2023), 'Civilian hackers blur the lines of modern conflict'.

to implementation of Principle 4 would then be 'know your customer' requirements, for intermediaries to ensure sellers are aware of their ultimate recipient. More indirectly, 'know your supplier' requirements, including knowledge of a supplier's other customers, could help states to prevent companies that sell to non-state actors from access to their markets. Some workshop participants supported this approach, with one explaining: 'We need to put the onus on the purchasers to understand the supply chain – knowing exactly who found it, where it is being sold, etc.' However, participants were more sceptical of models of trusted or licensed suppliers. One asked: 'What is trusted? A licensed company? Licensed researchers?' Another noted: 'If you have central, monopolized licences … this will kill creativity.'

A wider version of this principle would ask states to invest more in preventing and sanctioning actors who permit unpermissioned cyber intrusion on their territory, more akin to issues of due diligence. However, such expanded anti-hacking policies are beyond the scope of this paper, even though individuals (such as those using stalkerware in technology-facilitated abuse) or companies (such as private investigators or firms engaging in corporate espionage or aggressive public relations strategies involving hack-and-leak operations) are frequent users of unpermissioned cyber intrusion. Furthermore, such efforts would likely conflict with Principles 2 and 3 if national laws – or the implementation of treaties such as the UN Cybercrime Convention – do not sufficiently exclude permissioned cyber intrusion or good-faith security research from their scope.

Principle 5: States should be transparent in acknowledging unpermissioned cyber intrusion for military, national security and law enforcement purposes.

While the aim of Principle 4 is to limit end users of unpermissioned intrusion to states, this principle seeks to make state uses of such capabilities more transparent. Without acknowledgment by states that they use these capabilities, the next two principles (6 and 7), on how such capabilities should be used, are worth relatively little, as states cannot usefully discuss constraints on an activity they do not admit to conducting. Ideally, this acknowledgment would be made in the public domain, in the manner of general declarations of possession and use of offensive cyber capabilities by some militaries.[49] Some workshop participants highlighted the distinction between different kinds of state users of unpermissioned cyber intrusion, expressing doubt that states would provide data on espionage, rather than military or law enforcement.

There if of course a tension here between the goal of state transparency and the risk of revealing detail about such capabilities that may compromise operations, and so this principle does not ask states to go beyond general declarations. Disclosures of other information, such as levels of spending, numbers of contractors or aggregate instances of use, would also contribute to overall transparency – again, to the extent that states can acknowledge these details

[49] For an example of a high-level, open discussion about possession and use of offensive cyber capabilities, see National Cyber Force (2023), *Responsible Cyber Power in Practice*.

without compromising their operations.[50] States could also look to increase transparency in other areas, for example in disclosing their reasons for intervention against specific companies or individuals, tying them to specific contraventions of international law and norms, or principles such as those suggested here.

However, some recent reports have suggested that some states not only operate without transparency, but also seek to actively frustrate others' efforts at increasing transparency.[51] Overall, as one workshop participant suggested: 'Getting them to admit to it does feel like a good first step.' This principle therefore links closely to Principle 7, on adopting agreed minimum standards and being seen to do so.

D. Raising standards for unpermissioned intrusion

Principle 6: States should integrate their practices of unpermissioned intrusion with their efforts to improve anti-corruption, security governance and rule of law.

Some state abuses of commercial cyber intrusion capabilities occur as a result of wider issues of corruption (commercial cyber capabilities obtained by inappropriate state actors), security governance (use of such capabilities for purposes beyond legitimate law enforcement and national security goals, such as transnational repression or extrajudicial killings) or rule of law (data provided by such capabilities circumventing or undermining established judicial procedures). Many states have committed to international legal standards in these areas, as well as to initiatives by international organizations and non-governmental organizations to strengthen these fields.[52] As one workshop participant noted: 'What we're missing is that the key underlying problem is that states themselves are not in compliance with human rights law … We need to ask what more can states do on their side to bring themselves more in line.'

Commercial suppliers of cyber intrusion capabilities to states, for unpermissioned uses, should integrate the use of these capabilities to initiatives on anti-corruption, good security governance and the rule of law. Other states can support this integration by working with suppliers to integrate minimum standards at the technological, contractual and interpersonal levels. Again, a prerequisite for implementation of Principle 6 is a robust 'know your customer' mechanism, without which suppliers cannot evaluate whether such sales adhere to this principle. Such a mechanism should ideally be more granular than lists of sanctioned or blacklisted countries: it should identify specific departments or institutions within countries

[50] Some states already do this as regards numbers of counterterrorism targets, or numbers of live investigations. The more states can provide specific details, the less likely they are to face unexpected disclosure of their operations by cybersecurity researchers. For a pertinent example, see Howell O'Neill, P. (2021), 'Google's top security teams unilaterally shut down a counterterrorism operation', *MIT Technology Review*, 26 March 2021, https://www.technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally.
[51] Davies, H. and Kirchgaessner, S. (2024), 'Israel tried to frustrate US lawsuit over Pegasus spyware, leak suggests', *Guardian*, 25 July 2024, https://www.theguardian.com/news/article/2024/jul/25/israel-tried-to-frustrate-us-lawsuit-over-pegasus-spyware-leak-suggests.
[52] Among others, Transparency International's Corruption Perceptions Index (https://www.transparency.org/en/cpi/2023) and the World Justice Project's Rule of Law Index (https://worldjusticeproject.org/rule-of-law-index).

that would require additional scrutiny, and – conversely – those that implement best practices. Overall, this principle requires commercial cyber intrusion suppliers to work closely with civil society organizations both in and beyond the field of cybersecurity.

Principle 7: States should adopt OECD principles for government access to data, along with UN norms of responsible state behaviour, as minimum standards in their practices of unpermissioned intrusion.

This principle seeks to place commercial cyber intrusion capabilities in their broader context. It does so in two ways:

First, it recognizes that state unpermissioned use of such capabilities, especially for national security or law enforcement purposes, is one means among many of acquiring data, also including cooperative or coerced data requests from the private sector. While the legal and regulatory environment surrounding such data requests is significantly different to that around cyber intrusion capabilities, these are separate routes to similar end goals: (enforced) cooperation with a technology company to obtain 'passive' collection or access to its users' data; and adversarial access to users' data by compromising devices or products of that technology company without it or its users' permission (for example, using spyware). Although spyware can be more efficient at an individual level, providing a state with access to a wide range of data on applications run and managed by different companies for a single user, cooperative data requests can be more efficient at large scale, enabling data collection across multiple users.

In 2022, the Organisation for Economic Co-operation and Development (OECD) adopted a Declaration on Government Access to Data held by Private Sector Entities.[53] The purpose of the declaration is to establish principles for governments to request data from companies, especially multinational technology companies. These principles include: sound legal basis, legitimate aims, appropriate approval and handling, transparency, oversight and redress. The OECD principles, subject to some changes to allow for the different context, should be adopted as minimum standards for government use of unpermissioned cyber intrusion capabilities for data collection. If adopted, these principles would prevent many of the high-profile cases of misuse and abuse seen to date.

The difficulty here is in implementation. The OECD principles, in their original context, can theoretically be turned to by companies that are the subject of data access requests, thereby asking states to demonstrate their compliance with these principles before granting access. In contrast, the unpermissioned nature of access to data via cyber intrusion means that such companies cannot, by definition, ascertain whether these principles are in place. As one workshop participant noted: 'You could put all of the controls around [an exploit], but if someone doesn't want to follow them, you can't do anything about it.' Another suggested that 'end user licence agreements are hard to enforce in this space'. Instead, the burden is likely

[53] Organisation for Economic Co-operation and Development (OECD) (2022), 'Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access', press release, 14 December 2022. https://www.oecd.org/en/about/news/press-releases/2022/12/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.html.

to fall on the multi-stakeholder coalition working on broader improvements in security governance discussed in Principle 6, with many of the same potential implementation routes.

There is now a much wider understanding of the potential for state offensive operations, beyond data collection, occurring also in peacetime and involving non-military actors.

The second way in which this principle places commercial cyber intrusion capabilities in their broader context is to recognize that states do not only use them for data collection. They also use them for 'offensive' purposes – i.e. data deletion or manipulation intended to produce effects on connected cyber-physical systems or wider organizations and societies.[54] While such uses have predominantly been discussed in terms of military uses in conflict, there is now a much wider understanding of the potential for state offensive operations, beyond data collection, occurring also in peacetime and involving non-military actors.[55] Norms for such activity, including accepted and out-of-bounds targets, have been adopted as part of a framework for responsible state behaviour in cyberspace, developed through various UN processes.[56] State uses of commercial cyber intrusion capabilities for offensive uses should follow these principles, including their future elaboration. Some states, among them the UK, have already published documents detailing their interpretation of responsible state behaviour in the context of such operations.[57]

E. Avoiding non-commercial loopholes

Principle 8: States should apply, at a minimum, equally high standards to internal development and interstate transfer as they do to commercial activities.

This principle encourages states to apply Principles 6 and 7 equally to internal development and use of cyber intrusion capabilities, as well as to non-commercial transfers between states. While these two areas – internal development and interstate transfer – are very different, they are both non-commercial spaces not governed by the market dynamics discussed in this paper. Many states develop cyber intrusion capabilities in-house (i.e. within military, intelligence or law enforcement bodies), and sometimes transfer those capabilities via training, personnel movement or technology transfer to other states without a financial

[54] Moore, D. (2022), *Offensive Cyber Operations: Understanding Intangible Warfare*, London: Hurst Publishers.
[55] Fischerkeller, M. P., Goldman, E. O. and Harknett, R. J. (2022), *Cyber Persistence Theory: Redefining National Security in Cyberspace*, New York: Oxford Academic.
[56] See notably Hogeveen, B. (2022), *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN*, Australian Strategic Policy Institute, https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.
[57] National Cyber Force (2023), *Responsible Cyber Power in Practice*.

transaction.[58] Such transfers are governed largely by diplomatic considerations. The potential implementation of this principle is far less clear than the others, given the increased opacity of internal state activities compared with commercial ones. Nonetheless, it is crucial to mitigate the risks posed by misuse and abuse of cyber intrusion capabilities (commercial or otherwise), as the kind of interventions into the commercial market discussed in this paper potentially encourage states to take their development back in house and/or transfer capabilities bilaterally, outside market mechanisms. This principle seeks to pre-empt such unintended consequences.

[58] Smeets, M. (2022), *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, London: Hurst Publishers.

07 Conclusion

Achieving all-stakeholder consensus on key concepts of legitimacy and responsibility for cyber intrusion capabilities remains highly challenging. The principles set out in this paper are both sensitive to nuanced market dynamics, and keenly aware of the urgent need to prevent misuse and abuse.

This paper has proposed eight new principles for state approaches to commercial cyber intrusion capabilities. The principles are rooted in a new distinction between permissioned and unpermissioned cyber intrusion, which – despite complexities around overlapping supply chains and the breadth of activity contained on each side – offers a fresh entry point into a high-profile but polarized policy debate. While it will always be necessary to define and enforce standards of legitimacy and responsibility (indeed, Principles 6 and 7 go in this direction), trying to do so while treating both permissioned and unpermissioned intrusion together has repeatedly failed in the past, and may well fail in the future.

The key principles, then, are those that seek to separate the markets underlying these two kinds of intrusion (Principle 2), therefore enabling the stimulation of one market and not the other (Principle 3). Principle 1, on internal coherence, is a necessary condition of this separation and stimulation. Principles 4–7 are viable only if based on this separation; without it, efforts to limit end users (Principle 4), increase transparency (Principle 5), or raise standards (Principles 6 and 7) for unpermissioned intrusion are likely to run up against persuasive arguments that their negative impact is not worth the benefit. That is to say, such measures would restrict or stifle markets for permissioned intrusion that are currently crucial to improving global cybersecurity. Principle 8 is more speculative, seeing the potential for a shift away from commercial provision of cyber intrusion capabilities and endeavouring to ensure that such a shift does not lead to greater misuse.

These principles do not fit neatly within any existing policy initiative on commercial cyber intrusion capabilities. Rather, they are of relevance across multiple processes. At the UN, the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies is likely to include discussions on commercial cyber intrusion capabilities in the near future, while the use of such capabilities by law enforcement agencies makes them clearly relevant to the UN Ad Hoc Committee (AHC) on cybercrime. There are already linkage points with the OEWG in Principle 7, referencing norms of responsible state behaviour, as well as implications for discussions, within the AHC, on cybersecurity and cybercrime capacity-building – much of which takes place via commercial actors. The principles also offer avenues to strengthen export regulation while avoiding some of its negative impacts, thereby supporting signatories to the Wassenaar Arrangement and the EU Dual-Use regulation. And they provide high-level guidance and coherence for states that are already committed to substantial regulation and intervention, including via initiatives of the Summit for Democracy or the EU.

The principles' focus on exclusively state approaches – albeit with significant indirect impact on industry and other actors – inevitably means that they represent only a partial contribution to global multi-stakeholder or industry processes such as the Cyber Tech Accord, the Paris Call or the Pall Mall Process. However, achieving consensus across all stakeholders on key concepts of legitimacy and responsibility remains a highly challenging task. Until such a consensus emerges, these principles provide a way forward that can not only catalyse all states towards this broader goal, but do so in a way that is sensitive to the nuanced market dynamics of this field, and keenly aware of the urgent need to prevent their misuse and abuse.

About the author

Dr James Shires is a former senior research fellow in Chatham House's International Security Programme. He is currently the co-director of the European Cyber Conflict Research Initiative (ECCRI) and the European Cyber Conflict Research Incubator (ECCRI CIC).

James has conducted academic and policy research on commercial cyber intrusion capabilities for over a decade, including as the author of *The Politics of Cybersecurity in the Middle East* (Hurst, 2021), and as co-editor of *Cyberspace and Instability* (Edinburgh University Press, 2023).

Acknowledgments

The author and the International Security Programme at Chatham House are grateful for the support of the UK Foreign, Commonwealth and Development Office for funding this project and providing extensive feedback and guidance throughout the research phase. They are also grateful to the participants in the project's workshop, whose engagement and constructive comments and discussions were invaluable to shaping this paper. Finally, they thank colleagues from Chatham House, RUSI and ECCRI CIC for their contributions to the project.

Chatham House does not express opinions of its own. The opinions expressed in this publication are those of the author, and do not reflect the views of Chatham House, RUSI or any other institution.

Cover image: A Polish journalist's phone displays an alert warning that state-sponsored attackers may be targeting their device, on 7 March 2024 in Warsaw.
Photo credit: Copyright © Omar Marques/Contributor/Getty Images

ISBN 978 1 78413 627 7
DOI 10.55317/9781784136277

Cite this paper: Shires, J. (2024), *Principles for state approaches to commercial cyber intrusion capabilities: Navigating the policy challenges of cyber intrusion markets*, Research Paper, London: Royal Institute of International Affairs and RUSI, https://doi.org/10.55317/9781784136277.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223