Exploring the Regulation of Commercial Cyber Intrusion Capabilities' Proliferation and Misuse

Murdoch Watney
University of Johannesburg, South Africa

mwatney@uj.ac.za

Abstract: The commercial cyber intrusion industry has grown prolifically without any legal constraints for many years. Many governments and private clients contributed to the cyber intrusion capabilities' proliferation by paying millions of dollars to private companies for a variety of covert offensive cyber capabilities. The risk it presented to national security, rule of law and human rights' protection was not anticipated. Unchecked commercialisation of intrusion capabilities made its way to malicious state and non-state threat actors who would not have had access to it had it not been for the commercialisation. The harm resulting from the commercial development, selling, export and use of intrusion capabilities have contributed to make an already insecure digital ecosystem even less safe. Governments are exploring the regulation of commercial intrusion capabilities. The United States (US) government issued an executive order (EO) in 2023 banning the buying, export and use of commercial spyware on a domestic level that presents a risk to national security, rule of law, and human rights. Countries, such as the US, France and the United Kingdom (UK), took initiatives on a global level. The US issued a joint statement aimed at reigning in the proliferation of commercial spyware whereas France and the UK launched the Palm Mall Process in 2024 focussing on establishing norms that can serve as guidelines for the development and use of commercial intrusion capabilities. The discussion explores the necessity to regulate the commercial intrusion industry to ensure that digital intrusion capabilities are used in a responsible and human rights' respecting manner. The aim of regulating commercial intrusion capabilities is to make the digital ecosystem safer. The discussion evaluates the effectiveness of the initiatives to restrain the commercial intrusion industry, and prevent the misuse of these capabilities. The misuse of commercial intrusion capabilities constitutes an ongoing threat. Governments and companies must broaden their focus beyond controlling the commercial intrusion industry. They must extend their attention to cyber resilience and risk mitigation, and aim at having the necessary cybersecurity measures in place to prevent, detect, respond and recover from the malicious or irresponsible use of intrusion capabilities.

Keywords: Threat of unrestraint commercial cyber intrusion industry proliferation, Commercial cyber intrusion capabilities, Misuse of commercial intrusion capabilities, United States executive order on the prohibition of commercial spyware, Pall Mall Process on cyber intrusion tools

1. Introduction

The commercial cyber intrusion industry has for years been allowed to grow exponentially without any restrictions. In 2023, the United Kingdom (UK) National Cyber Security Centre (NCSC) warned that commercial cyber intrusion tools and services are doubling every ten years and with the expansion comes various serious risks to security and society (NCSC, 2023).

The commercial intrusion industry sold intrusion capabilities for a profit to governments and private clients which in return contributed to the prolific growth of the industry. At the time, governments did not anticipate the harmful consequences of the commercial development, selling, export and use of intrusion capabilities. In 2023 the UK Government Communications Headquarter (GCHQ) indicated that more than 80 countries had purchased spyware over the past decade (Baram, 2024). The procurement of the commercial spyware was not subjected to any oversight or control.

Intelligence agencies that developed in-house intrusion capabilities did not expect it to be disclosed to foreign governments and companies, and to be misused. For example, the 2017 WannaCry and NotPetya ransomware attacks used exploits originally engineered by the United States (US) (Herpig and Paulus, 2024; Landi, 2024). Ransomware is one of the most significant cyber threats currently facing the world. The use of commercial intrusion tools and services such as these zero-day exploits have been attributed to espionage actors, ransomware gangs, and financially motivated hackers (Landi, 2024).

Former government employees who received extensive training in the development and use of intrusion capabilities, moved on to become so-called cyber mercenaries who sell their technological expertise and state secrets to the highest bidder. Project Raven came to light in 2019 (Bing and Schetman, 2019). It consisted of a clandestine team that included more than a dozen former US intelligence operatives which were recruited to help the United Arab Emirates (AUE) engage in surveillance of other governments, militants and human rights activists critical of the monarchy. The operatives utilized an arsenal of cyber tools, including a cutting-edge

espionage platform known as Karma, in which Raven operatives hacked into the iPhones of hundreds of activists, political leaders and suspected terrorists (Bing and Shetman, 2019).

Intrusion capabilities have been linked to human rights abuses (Fidler, 2024). For example, spyware was used to monitor people close to Saudi dissident, Jamal Khashoggi, before and after his death (Fidler, 2024). Governments have used intrusive capabilities irresponsibly in cyberspace. In 2021, the US joined by allies and partners, namely the European Union (EU) and the UK, released a media statement criticising the irresponsible behaviour of the People's Republic of China (PRC) in cyberspace (US Whitehouse statement, 2021). It was alleged that hackers working for the PRC Ministry of State Security (MSS) had engaged in ransomware attacks, cyber extortion, crypto-jacking and theft from victims around the world for financial gain. Furthermore, PRC's MSS conducted cyber espionage operations utilizing the zero-day vulnerabilities in Microsoft exchange server disclosed in early March 2021.

It is against this background that the 2023 UK NCSC warning confirmed the serious concerns many governments, companies and other stakeholders have been voicing for some time, namely that the unrestricted commercial proliferation of intrusion capabilities poses a serious threat to democracy, rule of law and public safety within the ambit of the ever-growing cyber landscape. It allows state and non-state threat actors who would otherwise not have had the capability to develop or acquire intrusion capabilities, to obtain same, and misuse it.

Many governments agree that the proliferation should not be allowed to expand unchecked, and that the commercial intrusion industry should be controlled. Like-minded governments with other concerned stakeholders are exploring legal solutions to mitigate the threat commercial intrusion capabilities present for misuse.

The discussion focuses on the necessity for the regulation of commercial intrusion capabilities. The digital ecosystem is not secure, and the unrestrained growth of commercial intrusion capabilities has made it even less secure. Regulating the responsible use of intrusion tools and services with the focus on human rights' protection will make it safer. The discussion focuses on the following inter-related issues from a legal perspective:

- The US and the UK in collaboration with France are now taking steps to regulate commercial intrusion capabilities and have introduced two initiatives. The initiatives follow different approaches to regulation. The effectiveness of the approaches will be considered; and
- It should be determined whether the regulation of the commercial intrusion industry will curb the misuse of such capabilities.

2. An Overview of the Risk and Harm Commercial Cyber Intrusion Capabilities Present

Initially when commercial cyber intrusion capabilities were developed, the cyber landscape was not as extensively populated as it is today. The largest proportion of society lives and works in a borderless, interconnected, and inter-dependant digital world. As illustrated hereafter, the nature, and characteristics of the digital ecosystem, exacerbate the risk and harm caused by the malicious, irresponsible, or human rights disrespectful use of commercial intrusion capabilities.

- The malicious use of intrusive spyware can be detrimental to national cybersecurity as was illustrated by the 2021 US SolarWinds espionage (Temple-Rason, 2021). It was one of the most effective cyber espionage campaign in the US history. A major US software company, SolarWinds, was the subject of a cyberattack that spread to its clients, which may have started in 2019 but was only discovered in December 2020. Hackers, believed to be tied to the Russian government, gained access to SolarWinds systems and added a malicious code into the company's software system. The system, called Orion, is widely used by companies to manage IT resources. Orion updates, which included the hacked code, were received by as many as 18000 SolarWinds customers. The code created a backdoor to customer's information technology systems, which hackers then used to install even more malware that helped them spy on companies and organisations. The hacking campaign that infected numerous government agencies and tech companies with malicious SolarWinds software had also infected more than a dozen critical infrastructure companies in the electric, oil and manufacturing industries running the same software (Temple-Rason, 2021; Watney, 2022). The SolarWinds intrusion illustrates the importance of cybersecurity governance.
- Cybersecurity measures are not infallible. The malicious use of commercial intrusion capabilities for the commission of cybercrime is a major security concern and challenge for all countries on national and global level as it presents a serious threat to the security, confidence, and stability in cyberspace.

In many instances, cybercrime is committed cross-border, and the investigation involves international cooperation.

In 2024, UN member states at the Ad Hoc Committee (AHC) adopted the draft of the first globally binding legal instrument on cybercrime (UN Ad Hoc Committee, 2024). Once the UN General Assembly (UNGA) adopts the convention, a new global treaty addressing cybercrime with universal adoption across the entire UN membership will have a significant impact for users of information and communications technologies (ICTs). It would therefore bring greater security at national, regional and international levels. In particular, the convention aims to harmonise national approaches in fighting cybercrime and enhance international cooperation between states through developing clearer frameworks for investigation and cross-border data exchange. This convention would hopefully contribute to a more effective investigation that results in a prosecution.

- Misuse of cyber surveillance technologies designed to support law enforcement and intelligence objectives illustrates the double-edged nature of cyber surveillance (Handler, 2022).

Surveillance technologies have successfully been used by law enforcement and intelligence agencies for legitimate cybersecurity purposes. It has been shown to be an effective tool in the prevention and investigation of serious crimes subject to compliance with procedural and human right safeguards. The downside is that state and non-state actors have misused it for malicious purposes.

For example, one of the most high-profile spyware, created by the Israeli company, the NSO Group, asserts that the product it sells to government clients – most commonly referred to as Pegasus – is intended to "collect data from the mobile devices of specific individuals, suspected to be involved in serious crime and terror." It is a tool that can assist governments in the investigation of terrorists, paedophiles and other criminals. Pegasus has extensive capabilities and the spyware can be installed remotely on a smartphone without requiring any action from its owner. Once installed, it allows clients to take complete control of the device, including accessing messages from encrypted messaging apps like WhatsApp and Signal, and turning on the microphone and camera (Glover 2023).

It came to light that foreign governments used Pegasus spyware to target individuals, such as journalists and activists, and suppress dissent. In many instances, Pegasus has not been used for its intended law enforcement and security purposes, but it has been misused to spread authoritarianism, degrade human rights, and erode democratic values. It was for example used to illegally listen in on conversations in the UK government, via remotely accessing the then prime minister's phone (Glover, 2023). In 2023 it was revealed that 50 US government employees, based in the US and elsewhere, had been compromised by spyware (Kitchgaessner, 2024; Landi, 2024; Glover, 2023).

- There is a risk that not only authoritarian regimes, but also democratic governments may misuse intrusion cyber capabilities against their own citizens, including to surveil, and suppress activists, journalists, and political dissidents (Landi, 2024).

One of the most significant leaks in the US political history, was the 2013 revelations made by former US National Security Agency contractor, Snowden, in which he alleged that the US had conducted indiscriminate mass surveillance of terrorist suspects as well as US citizens (Fidler, 2024; Hardley, 2023). The revelations impacted negatively on the US as a leader in cybersecurity and upholder of democracy and protector of human rights.

- Intrusion capabilities are evasive. Encryption as a security measure has been a contentious issue with law enforcement and intelligence agencies requesting access to the encrypted data for investigatory purposes. In 2013, a killing took place in San Bernadino. During the investigation, the FBI requested Apple for access to the end-to-end encrypted communication on the iPhone belonging to the killers. Apple rejected the request citing that such decryption would weaken security and could be used by malicious threat actors (Nakashima and Albergotti, 2021). Ultimately, a vender developed and sold intrusion software to the FBI that unlocked the encrypted communication. If intrusion software is sold to a government to circumvent encrypted information, then that same software may be sold to a threat actor (Glover, 2021).

3. Initiatives in Constraining the Proliferation of Commercial Intrusion Capabilities

3.1 Discussion of the Initiatives

There is a necessity to restrict the commercial intrusion industry. It is commendable that the US and the UK in collaboration with France have responded to the proliferation of intrusion capabilities albeit with two separate

initiatives. In 2023 the US issued a joint statement on efforts to counter the proliferation and misuse of commercial spyware whereas France and the UK launched the Pall Mall Process (PMP) in 2024.

Both initiatives are aimed at securing a safer cyber landscape, but to achieve this aim, the initiatives follow separate approaches. The different strategies are explored hereafter to establish if the different approaches contradict each other and affect the usefulness of the two initiatives.

The US Approach: Specific action aimed at spyware

It is commendable that the US took the initiative and signed an executive order (EO) in 2023 banning the buying, selling, and use of commercial spyware that presents a risk to national security, rule of law, and human rights. The EO is significant as it is the first national buyer-side regulation pursued in the US (Fiddler, 2024b). It is not a blanket ban on the use of spyware (Swaney, 2023). Instead, it bars federal government agencies from procuring and using commercial spyware tools if they pose significant counterintelligence or security risks to the US government, or significant risks of improper use by a foreign government or foreign person, including the targeting of American citizens or enabling human rights abuses. The EO, for example, does not address the government's use of non-commercial spyware, such as government-produced spyware, or mention state or local government use of commercial spyware (Swaney, 2023). The US provides in its policy for specific government action that is aimed at limiting the use, sale, and procurement of commercial spyware that poses a risk. It enforces the restraint by means of economic sanctions, visa restrictions and export controls (Kitchgaessner, 2024; Landi, 2024). The US is hoping that the cumulative effect of the restrictions would result in limiting the spyware market currently available to malicious threat actors.

In 2023, at the second Summit for Democracy, governments released a US-led joint statement on efforts to counter the proliferation and misuse of commercial spyware. It recognises the threat posed by commercial spyware and the need for strict domestic and international controls on the proliferation and use for such technology. At the third Summit for Democracy held in 2024 additional countries became signatories to the joint statement (US-led joint statement, 2024).

The joint statement forms part of the broader US International Cyberspace and Digital Policy Strategy which aims to advance digital solidarity by working closely with allies and partners to ensure digital technologies are used in a responsible and rights-respecting manner.

The UK and France approach: creating a normative framework

The Pall Mall Process (PMP) aims to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities by means of a normative framework. It covers a wide segment of commercial cyber intrusion tools and services, such as hacking-as-a-service, hacker-for-hire, exploits of zero-day vulnerabilities and commercial spyware (Herpig and Paulus, 2024).

The initiative recognizes the legitimate uses for some of these intrusion capabilities. It does not "name and shame" actors who have a track record of abuse, but it aims to integrate international law, human rights law, and existing norms into a framework for the responsible use of cyber intrusion capabilities. The UK and France built the PMP on previous coalition-building initiatives, such as the Paris Call for Trust and Security in Cyberspace, the industry-led Tech Accord and the United Nation's framework for responsible behaviour in cyberspace (Landi, 2024).

It establishes principles and policy options for states, industry and civil society in respect of the various tools and services. The approach is based on a multi-stakeholders' model which includes a broad set of governments, civil society, the private sector and signatories to the initiative (Baram, 2024; Landi, 2024). It creates opportunities for commercial cyber intrusion companies to engage with governments, civil society, and other stakeholders (Baran, 2024).

The PMP highlights four activities to guide the formation of voluntary norms to tackle cyber intrusion capabilities proliferation, namely

1. holding states accountable when behaviour is inconsistent with international human rights law;
2. developing precise conditions for use;
3. implementing assessment and due diligence mechanisms for users and vendors; and
4. conducting business transactions with transparency.

3.2 Evaluating the Usefulness of the Initiatives

It is commendable that the US, France and the UK are exploring strategies to regulate commercial surveillance capacities. Many countries support the initiatives.

The following challenges have been highlighted:

- The initiatives focus only on commercial intrusion capabilities. The US narrowed its focus to commercial spyware whereas the PMP covers a variety of commercial intrusion capabilities which includes spyware. Focusing only on commercial spyware excludes the wider marketplace of surveillance and intrusion capabilities, such as exploit kits sold on the dark web. Countries may agree to regulate the use of commercial spyware tools, but continue to purchase other exploits from the vulnerability market. The uncontrolled use of such exploits present a threat to national security (Landi, 2024). The wide range of cyber intrusion capabilities requires an equal level of governance and prioritisation.
- The initiatives exclude governments that develop their own intrusion capabilities, as well as companies that exclusively cater to governments (Herpig and Paulus, 2024; Landi, 2024). Herpig and Paulus (2024) question the exclusion of non-commercial intrusion capabilities, dual-intent tools and freely available exploits. The organisers of the PMP may have decided to limit the regulation to commercial intrusion capabilities to make the process easier to create, and implement (Herpig and Paulus, 2024).
- A country must have the commitment and political will to restrict commercial intrusion capabilities. In this regard, the US is taking concrete action on a domestic level by means of sanctions, visa restrictions and export controls to ensure that commercial spyware that presents a threat to cybersecurity, rule of law and human right protection are not used, sold or exported. Landi (2024) opines that the spyware sanctions are an important move by the US, and its EO, export controls, and visa restrictions have built significant momentum for targeting the commercial spyware industry. The US however, cannot keep this momentum going on its own and need the support from its allies in taking similar action in regulating commercial spyware.
- Landi (2024) opines that the UK-France initiative risks advancing a largely symbolic strategy bolstering long term norms without much real-world progress. She observes that neither France nor the UK has passed their own restrictions against the commercial hacking industry on a domestic level. Furthermore, various authors, such as Feldstein and Kot (2024), Landi (2024) and Fidler (2024) opine that the European Union's (EU) strict regulations around the sale of spyware have not prevented spyware vendors from taking advantage of states who ignore violations or refuse to enforce regulations. For example, Greece, Spain, Hungary, and Poland used spyware on domestic political opposition groups. As a result, the EU has become a breeding ground for the development and sale of commercial spyware (Fedler, 2024; Landi, 2024).
- Although the PMP has a lot of supporters, Herpig and Paulus (2024) opine that it may have sacrificed substance in exchange for a larger base of supporters. They are of the opinion that if the PMP wishes to make substantial progress in developing guidelines for the use and spread of commercial cyber intrusion capabilities, then like-minded countries of liberal democracies should work together. The current circle of supporters may include countries that have transgressed human rights, but such a country may now commit to the use of intrusion capabilities in a responsible and human rights respectful manner. The issue at hand is establishing an ongoing, inclusive global dialogue between countries and other stakeholders in order to reach a common understanding of what constitutes responsible behaviour in cyberspace in respect of the development and use of commercial intrusion capabilities.
- The US-led joint statement and the PMP are encountering a common challenge seen in the past to regulate cyberspace, namely an absence of harmonised action and responses.

Landi (2024) opines that the Joint Statement and the PMP have the potential to complement each other. The author proposes that the approaches should be harmonised into one cohesive approach which will provide for better accountability, clearer criteria for best practices and increased pressure on misbehaving actors.

- Reaching a global agreement on the norms applicable to the responsible and human rights' respecting development and use of commercial intrusion capabilities will be a complex process as was shown with the adoption of the Cybercrime Treaty by the UN AHC. It was a lengthy process preceded by ten rounds of negotiations, complete with a reconvened concluding session, as the states could not come

to an agreement at the original concluding session. As the name, PMP, suggests, the process foresees a series of steps, including a 2025 follow-up conference.

4. Recommendations

Although the regulation of commercial surveillance capabilities presents challenges, the challenges can be mitigated.

- The complete ban of the development, selling and use of commercial intrusion capabilities will not be successful. Swaney (2023) correctly opines that the pandora's box of commercial spyware has already been opened. The commercialisation of intrusion capabilities cannot be reversed, but the risk and harm associated with it can be managed.

There is a demand for commercial intrusion tools and services which has resulted in the industry being worth over an estimated $12 billion (Fidler, 2024). Governments and law enforcement agencies are prime customers, but this demand is also driven by states that lack technical expertise and resources necessary to develop their own offensive cyber capabilities, and rely on the commercial surveillance industry to keep pace with national adversaries. Therefore, the banning of all commercial surveillance technologies will result in an industry that will continue to exist and most probably flourish, but in secrecy.

- The banning of procuring and using of commercial spyware that present a risk to national security or for improper use does not eliminate the security risk associated with it as a threat actor, such as another state or a non-state cybercriminal, may still use it for malicious purposes. However, the restrictions imposed by the US EO may make it challenging for the malicious threat actor to procure the technology. Countries on a domestic level should consider following suit, and imposing restrictions in respect of commercial intrusion capabilities.
- The US Department of Commerce has an entity list which is a trade restriction list consisting of entities that engaged in activities contrary to the national security or foreign policy interests of the US (Herpig and Paulus, 2024). The US Office of Foreign Assets Control also has a specially designated nationals list and the individuals and entities on the list have their assets blocked. US persons are prohibited from dealing with them (Herpig and Paulus, 2024).

Fernstein and Kot (2023) recommend that the US entity list is multilateralised. They opine that the US should pressurise EU member countries to set up a parallel entity and to similarly sanction, for example, the NSO Group, Candiru and related firms. Although there is merit in their recommendation, the multilaterisation and pressure should be exerted on a global or international level. When a specific country makes unilateral demands, it may result in geopolitical tension.

- Public investigations of commercial vendors and buyers as well as advocacy campaigns have been effective, such as the US blacklisting of the NSO group in 2021 and the financial impact the blacklisting had on the company. The action by the US government against a commercial vendor who sells its capabilities, for example, to an authoritarian government that violates human rights, shows that the US government is serious in tackling the misuse of commercial surveillance technologies. Although the demise of a surveillance vendor does not mean that another will not take its place, it shows vendors that they will be held accountable of the way the buyer uses the surveillance technology.
- The proposed norms of the PMS (discussed at par. 3) could be given consideration on a national level in respect of the development, use, export, and sale of commercial intrusion capabilities.
- The use of surveillance technologies on a national level by law enforcement and intelligence agencies should be re-visited on a regular basis. It is an effective tool for the prevention or investigation of a specific serious crime or an act constituting a grave threat to national security, but it must comply with various procedural and human rights' safeguards. International law holds that targeted surveillance measures should be narrowly tailored to investigate specific individuals suspected of committing serious crimes or acts threatening national security (Feinstein and Kot, 2023). Spyware should be deployed as a last resort and the duration and scope of spyware use should be strictly limited only to relevant data. In short, governments should comply with the principles of "legality, necessity, and proportionality" when using cyber surveillance technologies.
- The discussion shows that intrusion capabilities can be misused for the commission of cybercrime. Technical, legal, and human centred cybersecurity measures on a national level play a crucial role in pro-actively mitigating the threat commercial intrusion capabilities poses. If security measures are violated, then due diligence and resilience should be key to recovering from such a breach.

5. Conclusion

The discussion highlights that governments who contributed to the growth of commercial intrusion capabilities, did not anticipate the risk and harm of the commercial cyber capabilities' proliferation. The unchecked commercialisation of intrusion capabilities has made an insecure cyber ecosystem even less safe.

The consequences of the unrestricted proliferation of commercial intrusion tools and services cannot be reversed, but going forward the harm and risk can be mitigated. The first step in the regulation of commercial intrusion capabilities should be on a domestic level by means of action and response. The development, selling, export and use of commercial intrusion capabilities must be subjected to accountability, oversight, and transparency. The approaches of the US-led joint statement and the PMP are welcomed, but it should be harmonised into a cohesive framework that outlines norms for the responsible and human rights' respectful development and use of commercial intrusion capabilities on a global level.

The takeaway from the discussion is that the cyber ecosystem is vulnerable to risk and harm. Governments, private companies, and the public must take security measures to mitigate the risk and harm that arise from the malicious, or irresponsible or human rights' disrespectful use of commercial intrusion capabilities.

References

Baram, G, (2024) The Pall Mall Process could be a catalyst for international collaboration on commercial cyber intrusion capabilities", [online], https://bindinghook.com/articles-hooked-on-trends/the-pall-mall-process-could-be-a-catalyst-for-international-collaboration-on-commercial-cyber-intrusion-capabilities/.

Bing, C., and Schetman, J. (2019) [online], "Project Raven: Inside the UAE's secret hacking team of American merceries", [online], https://www.reuters.com/investigates/special-report/usa-spying-raven/.

Feldstein S. and Kot, B. (2023) "Why does the global spyware industry continue to thrive? Trends, explanations and responses", [online], https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en.

Fidler, M. (2024) "Zero Progress on Zero Days: How the Last Ten Years Created the Modern Spyware Market" 102 Neb. L. Rev. 713 (2024), [online], https://ssrn.com/abstract=4626426.

Glover, C. (2021) "Spyware threatens both human rights and cybersecurity", [online], https://www.techmonitor.ai/technology/cybersecurity/pegasus-spyware-cybersecurity?cf-view.

Glover, C. (2023) "US government banned from using spyware like Pegasus", [online], https://www.techmonitor.ai/technology/cybersecurity/spyware-us-government-joe-biden-pegasus.

Handley, P. (2023) "Snowden leaks: 10 years later, US intelligence still collects huge amounts of information", [online], https://mg.co.za/world/2023-06-05-snowden-leaks-10-years-later-us-intelligence-still-collects-huge-amounts-of-information/.

Handler, S. (2022) "The 5x5-The rise of cyber surveillance and the Access-as-a-Service industry", [online], https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-rise-of-cyber-surveillance-and-the-access-as-a-service-industry/.

Herpig, S., and Paulus, A. (2024) "The Palm Mall Process on Cyber Intrusion Capabilities", [online], https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities.

Joint Statement to Counter the Proliferation and Misuse of Commercial Spyware. (2024) [online], https://www.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

Kitchgaessner, S. (2024) "US announces new restrictions to curb global spyware industry", [online] https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions.

Landi, E. (2024) "Harmonizing recent campaigns to tame the hacking marketplace", [online], https://carnegieendowment.org/r USesearch/2024/06/us-europe-cyber-policy-joint-statement-pall-mall-process?lang=en.

Nakashima, E., and Albergotti, R. (2021) "The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm", [online], https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/.

Swaney, R. (2023) "Will commercial spyware survive Biden's executive order?", [online], https://securityintelligence.com/articles/will-commercial-spyware-survive-bidens-executive-order/.

Temple-Rasten, D. (2021) "A worst nightmare cyberattack: The untold story of the SolarWinds Hack", [online], https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

United Kingdom (UK) National Cyber Security Centre (NCSC). (2023) "The threat from commercial proliferation", [online], https://www.ncsc.gov.uk/report/commercial-cyber-proliferation-assessment.

United Kingdom Foreign, Commonwealth and Development Office. (2023) "Efforts to counter the proliferation and misuse of commercial spyware: joint statement", [online], https://www.gov.uk/government/news/efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware-joint-statement.

United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. (2024 [online], https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

United States International Cyberspace and Digital Policy Strategy. [online], https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

United States Whitehouse Executive Order. (2023) "Executive order on prohibition on use by the United States Government of commercial spyware that poses risk to national security", [online, 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/.

United States-led Joint Statement. (2021) "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behaviour to the People's Republic of China", [online], https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

Watney, MM. (2022) "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective", Proceedings of the 21st European Conference on Cyber Warfare and Security, [online], https://papers.academic-conferences.org/index.php/eccws/article/view/196.