Public Attribution in Cyberspace: Symbolic Gesture or Strategic Weapon?

Mihai OLTEANU
National Defense University "Carol I", Bucharest, Romania
mihaiolteanu48@yahoo.com

Abstract

States have developed multiple defensive approaches, but deterrence has emerged as a central element of cyber strategy. Public attribution (the official act of publicly identifying the actor responsible for a cyber operation) has become a widely used instrument, particularly among NATO and EU members, despite its high political and technical costs. This paper examines the relationship between public attribution and deterrence, with reference to five recognized forms: punishment, denial, entanglement, norms, and association. Using recent data and selected cases, the analysis shows that public attributions can sometimes generate tangible outcomes (e.g., sanctions, indictments, or defensive improvements), while in other cases they produce little deterrent effect. Nonetheless, the value of public attribution should not be measured solely by utilitarian efficiency, but also through the principled lens of international law and normative signaling. Even when immediate effects are absent, attribution reaffirms international norms, imposes reputational costs, and prevents the normalization of hostile behavior in cyberspace.

Index terms: Advanced Persistent Threat, cybersecurity, deterrence, international law, public attribution

1. Introduction

The last two decades have witnessed a continuous growth in the number of cyberattacks, characterized by diverse technical features, varying levels of complexity and innovation, and a substantial number of victims worldwide. Notably, since 2013, the main area of interest of cyberattacks has shifted constantly, from operations focused on cloud computing (2013), Internet of Things (2014), cryptocurrency (2017), and the healthcare system (2019-2020), to campaigns that reflected the rise of Artificial Intelligence in automating and accelerating attacks [1], highlighting a connection between cyberattacks and emerging technologies.

While the overall landscape of cyberattacks has evolved rapidly in scope and focus, Advanced Persistent Threats (APT) campaigns represent a somewhat distinct phenomenon. Although these operations account for a smaller share of the total incidents compared to financially or ideologically motivated attacks, APT operations remain the most relevant threat in terms of strategic impact for both states and companies, as their outcome is likely to fundamentally affect the activity of these entities. APT campaigns have evolved their tools but have also remained stable in terms of core characteristics (e.g., long-time persistence, highly-tailored targeting of specific domains, and significant funding) and modus operandi [2].

In dealing with APT campaigns, multiple techniques and procedures have been developed by state agencies and private companies, focused on each level of decision: strategic, operational, and tactical. Tactically, the defensive mechanisms evolved by integrating tools such as Intrusion Detection

Systems and Endpoint Detection and Response systems, while operationally, the use of advanced tools for anomaly detection and behavioral analysis strengthened the security of the systems [3]. Still, strategically, the practice of deterrence in cyberspace has remained a continuous component in handling massive APT campaigns. Such an approach is rather specific to governments, as private companies are more oriented towards financial gains, instead of strategic statements and international sanctions.

The practice of deterrence is the result of a set of strategic approaches that ultimately aim to discourage the threat actor from conducting campaigns against a target or a group of targets [4]. The effectiveness of traditional deterrence strategies is directly dependent on technical arguments that outline the identity of the author of a cyberattack, a process generally referred to as attribution. Naturally, the aim of different states to impose various deterrence measures requires, in most cases, a previous attribution of a cyber campaign, which usually becomes public if enough data is gathered, to serve as a foundation for additional diplomatic, economic, or technical measures. By officially identifying and exposing the responsible actor, governments attempt to impose reputational costs, reduce the adversary's room for plausible deniability, and mobilize international support against common threats [5].

During the last decades, public attribution of cyberattacks has become a traditional tool in dealing with cyberattacks, with examples dating back to 2007 (Estonia to Russia [6]), 2010 (Google to China [7]), and 2014 (USA to North Korea [8]). However, there are constant debates surrounding the efficiency of such approaches, considering the various reactions of the threat actors after the public attribution is conducted.

This paper aims to analyze multiple approaches to public attribution of cyberattacks, looking to provide arguments for and against this process, from a utilitarian perspective. In doing so, several deterrence mechanisms will be evaluated, along with some examples of public attributions and the outcomes they generated. Considering that this approach is rather specific to governments, as it is a predecessor of other diplomatic or technical actions, in accordance with international law, the public attributions performed by private companies will not be discussed in this paper.

2. Deterrence in cyberspace

The persistence of APT campaigns, as well as the high stakes implied by such operations, oblige governments to address the matter by exploiting a mixture of decisions on each of the three levels. Therefore, while tactical and operational approaches mainly resemble financial investments, strategic decisions are usually focused on various deterrence mechanisms, shaped to generate expected behaviors from threat actors.

Joseph S. Nye described deterrence as a set of means that dissuade adversaries from conducting operations by making them believe that the expected benefits are exceeded by the most probable costs [9]. Deterrence is only useful if, psychologically, all the actors involved calibrate their perceptions regarding the costs and benefits. The most reliable example of deterrence that serves such a definition is the one regarding the nuclear threat, which implies a set of outcomes that makes any attempt at such conflict seem unworthy.

The author further described four approaches to this strategy: (1) deterrence by punishment, where the retaliation is likely to produce unwanted or unacceptable damage to the initiator of the attack, thus making the initial offensive unfit; (2) deterrence by denial, essentially consisting of building the required capabilities to prevent or limit the damage, therefore convincing hostile operations that their chances of success are reduced; (3) deterrence by entanglement, which implies that the aggressor and the victim are so well interconnected that an attack against the latter is likely to produce damages also against the former, concluding to a financially unfeasible situation and (4) deterrence by norms, implying a reputational damage to the aggressor, as the break of international

rules may affect its soft power capabilities in the medium and long run [9]. The variety of deterrence strategies implies that not each one of them works for any type of aggressor, as some might be more preoccupied with their international reputation (e.g., China [10]), and some with the retaliation, given that their cybersecurity level is rather low.

N.J. Ryan provides a complementary perspective by adding a fifth mechanism, deterrence by association, a term initially used by Paul Cornish. His theory essentially states that the risk of being connected with the outcomes of a significant cyberattack through public attribution is a setback both for governments, which may face different types of strategic consequences, such as public condemnation, and for individuals, who could be indicted [11]. Such cases have been constantly identified, with several American public attributions directly naming some individuals who conducted cyber operations and are being legally pursued for crimes such as conspiracy to damage protected computers, economic espionage, identity theft, or conspiracy to commit computer intrusions [12] [13] [14].

Out of the five types of approaches, deterrence by denial and deterrence by entanglement are indifferent to the existence of an attribution, be it public or classified. However, it could be argued that these two categories also pose the lowest level of deterrence, as the first one is purely based on a financial analysis, concomitantly with the fact that some of the most evolved defensive mechanisms have eventually been breached. The second one is also based on an economic calculus, and could easily be overcome if the benefits obtained in a sector are more relevant than the damage produced by the existence of an interconnectivity in another. For instance, if compromising an interconnected portion of an energy network would generate immediate military advantages, such as control over essential areas, the cyber operations may seem to produce sufficient benefits to justify their existence and the final damage.

The other three deterrence mechanisms are directly linked to the preexistence of an attribution process, generally joined by at least a small degree of declassified details, that would publicly and internationally justify retaliation, normative punishment, or reputational damage through association with the authors of the operation. Therefore, a link between publicly attributing a cyber operation and most of the existing deterrence measures is evident, as any statement or action has to be based on some degree of evidence. Attribution becomes the enabling condition, since without a credible identification of the attacker, no measure can be effectively targeted. At the same time, the act of public attribution in itself functions as a deterrent by exposing the adversary, reducing plausible deniability, and signaling collective resolve to broader audiences.

3. Public attribution of cyberattacks

The public attribution of a cyberattack refers to the official act of publicly naming the actor deemed responsible for an operation, often based on a combination of technical forensics, intelligence assessments, and strategic considerations. The act of publicly attributing a cyberattack can take place in various ways, mainly ranging from public statements made by governments or institutions to joint communiqués performed by a set of international partners [15].

Generally, the public attribution of a cyberattack requires a consistent set of technical, financial, and political resources. Therefore, inherently, the investment of such an amount of resources has to be justified by an outcome that produces proportional advantages [16]. In this sense, public attribution is rarely employed for opportunistic or cybercrime activities, but rather for APT campaigns, which are typically state-sponsored, long-term, and strategically significant. The persistence, geopolitical relevance, and high-value targets of APTs make them the most likely category of operations to warrant the political and strategic effort of an attribution [17].

The European repository for Cyber Incidents distinguishes between five types of attributions performed by different entities [18]:

- Technical attribution, meaning the assignment of technical responsibility for a cyber incident by analyzing the attackers' tactics, techniques, and procedures to infer the likely origin of the operation. Such an attribution is rather specific to private cybersecurity companies, which publish such technical reports regularly, as part of their usual activity [19].
- Unofficial Policy Attribution, the process of attribution of responsibility for a cyber incident that may include statements or leaks from public officials or senior civil servants reported in the media.
- Official Policy Attribution, based on public statements, press releases, or speeches by government officials or senior civil servants. Unlike technical or legal attribution, this form of attribution generally presents less direct evidence and may emphasize political or strategic considerations. This is the most common form of public attributions performed by states.
- Legal Attribution, the process aimed at prosecution or the formal declaration of a violation of legal norms. It typically involves presenting verifiable evidence and supporting documentation to substantiate the claim. Such examples include extensive and complex technological investigations that typically end with naming not only states or agencies, but also individuals.
- Self-Attribution, a process conducted by the perpetrator, such as hacktivists or cybercriminals, often via social media or other public channels. Motivations for such disclosures may include intimidating the victim, signaling capabilities, or increasing pressure in the context of ransomware or extortion operations [18].

Considering that this study is focused on public attribution as a component of deterrence, we will mostly focus on the Official Policy Attribution, as it is the most common outcome of the efforts of a government towards naming a foreign perpetrator that managed to compromise its networks and produce damage.

The public attribution itself is a complex process, difficult to correctly and completely argue, given the nature of cyberspace, known for its volatility and high degree of anonymity. Compared with traditional means of deterrence, the public attribution of cyberattacks faces additional challenges. For instance, when discussing deterrence in the nuclear field, the limited number of states that possess such an arsenal is sufficient to limit the list of possible perpetrators [9]. Other attribution processes focused on the military area could be correctly argued through tangible evidence, such as pictures or recordings, while this is not the case for cyberattacks.

Given the high investments required to perform public attribution in cyberspace, as well as the difficulty in gaining strategic advantages through deterrence mechanisms, a further analysis of the efficiency of such processes is required.

4. Evaluating the public attribution

According to data published by the European Repository of Cyber Incidents on September 26, 2025, there have been 1,617 public attributions of all five types worldwide since 2022, with 704 of these being self-attributions. Therefore, there were 902 technical, legal, unofficial, and official policy attributions during the last five years, out of which:

- 215 (approx. 23.8%) have pointed to Russian private or governmental entities as being the authors of the attacks.
- 167 (approx. 18.5%) have indicated Chinese private or governmental entities as being the authors of the attacks.
- 107 (approx. 11.8%) have pointed to North Korean entities as being the authors of the attacks.

- 91 (approx. 10%) have indicated Iranian private or governmental entities as being the author of the attacks [18].

Therefore, 64.1% of all public attributions conducted over the past three years identified traditional NATO and EU adversaries as the perpetrators of cyberattacks. This distribution suggests that public attribution is regularly used as a strategic instrument against adversaries in cyberspace by EU and NATO members. By attributing cyberattacks to adversarial states, NATO and EU members reinforce a narrative of external threats, thereby justifying defensive policies, strengthening alliances, and deterring future aggression [20].

More specifically, since 2022, out of the total of 902 public attributions, the most have been initiated from:

- US, 391 attributions (approx. 43.3%).
- EU states, 151 attributions (approx. 16.7%).
- Ukraine, 57 attributions (approx. 6.3%).
- UK, 42 attributions (approx. 4.6%) [18].

The fact that the majority of public attributions (64.6%) are issued by NATO and EU states highlights important dynamics. These data demonstrate the political will and strategic approach of the Western states, as the attribution is not solely a technical act but also a political choice, and NATO/EU members have consistently employed it as a tool of deterrence and signaling [21].

However, public attribution has also been employed by adversarial states through different approaches. On one hand, China has made limited use of this tool, issuing only 13 public attributions over the past three years. On the other hand, Russian entities have conducted 157 public attributions, the majority of which (119 cases, 75.7%) were self-attributions, typically made by hacktivist groups that publicly claimed responsibility for cyberattacks [18].

The asymmetry between NATO/EU members and Russian attribution practices is significant. On the Western side, the majority of public attributions target Russia, portraying it as the primary source of malicious cyber activity and reinforcing its image as a systemic threat. This reflects a deliberate strategic use of attribution as a tool of deterrence. By contrast, most Russian attributions are not directed but are instead self-proclaimed, with hacktivist groups claiming responsibility for attacks. In this sense, public attribution in the Russian context operates less as a mechanism of assigning external responsibility and more as an act of demonstrating its capabilities.

Ukraine represents a hybrid case, which seems to combine elements of both Western and Russian practices, as it has issued 120 public attributions, of which more than half (63, approx. 52.5%) are self-attributions. On one hand, Ukraine engages in outward-facing attribution, using public attribution as a strategic tool for naming and shaming. On the other hand, the significant proportion of self-attributions (often claimed by Ukrainian hacktivists or even governmental institutions) reflects a strategy where self-proclaimed operations are used to project resilience, demonstrate offensive capability, and, possibly, sustain domestic and international morale during wartime.

Still, the efficiency of public attribution is debatable. There have been cases that illustrated several outcomes produced by such initiatives, indicating that the strategic use of public attribution has been a relevant tool. In 2021, a worldwide campaign dubbed HAFNIUM revealed the exploitation of several zero-day vulnerabilities in Microsoft Exchange servers, affecting a variety of industries, with an estimated number of more than 30.000 in the US alone, and hundreds of thousands globally [22]. While Microsoft released several statements on this matter, along with a set of patches to prevent further exploitation of the zero-day vulnerabilities [23], there was a continuous growth in the number of victims. In July 2021, the UK, alongside international partners, issued an official public attribution holding Chinese state-backed actors responsible for the exploitation of Microsoft Exchange Server vulnerabilities. The UK's National Cyber Security Centre assessed with high confidence that the group HAFNIUM was almost certainly affiliated with the Chinese state and that the operation was

likely intended to enable large-scale cyber espionage. The UK also called on China to adhere to its 2015 G20 commitment not to engage in cyber-enabled intellectual property theft [24].

While the attribution itself did not lead to deterrence by retaliation, by entanglement, or by denial (as, by the end of March 2021, 92% of the potential victims patched the vulnerabilities [24]), it posed, however, several elements indicating deterrence by association and by normative taboos, proving a relevant level of efficiency. Precisely, this initiative functioned as deterrence by association, considering that China felt obliged to issue a response to the public attribution, in which it firmly denied and called these claims unreasonable [25]. Moreover, deterrence by normative taboos functioned by exposing and denouncing state behavior that did not follow established cyber norms (particularly focused on large-scale espionage and the theft of intellectual property). Even without immediate punitive consequences, the act of public shaming contributes to long-term normative pressure against such conduct. Moreover, the official response of the Chinese authorities pointed out that the country is committed to these norms by opposing and condemning any form of cybercrime [25].

Similarly, other public attributions managed to produce some forms of deterrence, such as the one initiated by the US in March 2024, naming and sanctioning a group of defendants that were linked to the cyber operations conducted by APT31, a threat actor publicly attributed to the Chinese Ministry of State Security [26]. Similarly, France's individual public attribution of APT28's operations to the Russian military intelligence service marked a notable precedent, being the first such attribution issued independently by France against Russia [27]. It also produced important outcomes aiming to improve deterrence by denial by using this public attribution as an argument to update its strategic view (that, unlike other versions, explicitly points out Russia as the primary threat) [28] and to task the ANSSI (Agence nationale de la sécurité des systèmes d'information) to strengthen the national cybersecurity [29].

On the other side, there are examples of public attributions that did not produce an important outcome in terms of deterrence. Simply evaluating the high number of public attributions conducted during the last three years points out that the mechanism has become a common tool used mostly by EU or NATO states to publicly shame a threat actor. For instance, while APT SANDWORM has been constantly blamed and shamed for conducting cyberattacks against European infrastructures [30] [31], its operations continued, managing to compromise a consistent number of victims. This suggests that while public attribution has become a widely and often used instrument, it does not inherently produce quantifiable strategic outcomes of any kind, as adversaries react differently to similar incentives. However, from a tactical perspective, the public attribution of an ongoing cyberattack can function as a form of deterrence by denial, as it signals that the intrusion has been detected and forces the perpetrator to change and adapt its techniques [17]. This, in turn, imposes additional costs in terms of time, manpower, and resources.

5. Conclusions

The analysis of public attribution of cyberattacks demonstrates that this mechanism has become a common and visible instrument in the cyber field, particularly among NATO and EU members. However, its efficiency as a tool of deterrence is not uniform. Certain cases, such as the public attribution of HAFNIUM and APT31, illustrate that public attributions can generate strategic outcomes (e.g., international accusations, improvement of defensive capabilities) or even tangible ones (e.g., indictments). In contrast, other instances, such as the repeated attributions against APT SANDWORM, might indicate little effect in preventing further hostile cyber operations, as the perpetrators continued their activities.

Still, this variation of outcomes highlights that public attribution should not be assessed solely through the lens of utilitarian efficiency. While deterrence by denial, punishment, norms, retaliation,

or entanglement may sometimes be achieved, the act of attribution carries value even in the absence of immediate strategic outcomes. Public attribution reaffirms international principles, signals consistency in policy, and serves as a normative act of designating unacceptable behavior [21]. In this sense, it functions as much as a political and moral statement as it does as a practical deterrent. Moreover, the failure to attribute would risk normalizing hostile cyber operations and signaling acceptance of such behavior.

Furthermore, the distribution of public attributions in recent years underlines the political dimension of this practice. The majority of attributions have been performed recently by a relatively small group of states (mainly the US, EU members, the UK, and Ukraine). Russia and China, by contrast, employ this tool only rarely and in distinctive ways. Chinese authorities have issued very few official public attributions, while Russian practices are dominated by self-attributions claimed by hacktivist groups, often with the purpose of intimidation, propaganda, or boasting of capabilities. Russia's decision to use self-attribution less as a mechanism of external accountability and more as a performative act of demonstration highlights that public attribution can sometimes become a form of strategic communication [21], shaping perceptions of legitimacy and responsibility in cyberspace. Taken together, these practices suggest that Russia uses indifference to public attribution as a strategic posture, signaling resilience and trying to diminish the credibility of attribution as a deterrent tool. Still, at a minimum, public attribution signals that actions presumed to remain hidden have been uncovered, obliging the actor to reassess its operational security and tactical approach, hence requiring investments [17].

Ukraine, positioned in the middle of these approaches, has combined Western-style naming and shaming with a significant proportion of self-attributions, particularly during wartime. Its objective might be to signal resilience, deterrence, and offensive capacity to both domestic and international audiences.

Finally, while not all public attributions are effective in producing direct deterrent outcomes, their broader value lies in their cumulative and symbolic impact. Repeatedly attributing hostile cyber operations to adversaries contributes to long-term reputational costs and strengthens normative taboos. Even in cases where immediate deterrence is absent, attribution remains necessary to uphold international norms, maintain consistency, and avoid the erosion of standards in cyberspace. The act of attribution, therefore, should be understood not only as a utilitarian tool but also as a principled practice.

6. Discussions

This paper does not argue against the practice of publicly attributing cyber operations; on the contrary, it advocates for its continuation, as it reinforces existing norms, highlights the responsible actor, and signals unacceptable behavior in cyberspace. The main argument that can be extracted from this paper is that public attribution should not be assessed solely in terms of efficiency, but rather through the principled lens of international law, which obliges states to act against perpetrators even when such actions do not produce measurable effects, but serve to uphold valuable international norms.

However, a quantitative analysis assessing the effectiveness of public attributions in supporting each of the five forms of deterrence could provide a conclusive perspective on this discussion. Moreover, such an analysis should differentiate between types of aggressors, as their responses to public attribution are likely to vary depending on domestic dynamics and international strategies or behaviors.

Nevertheless, regardless of the outcomes of such assessments, the principle of publicly attributing a cyberattack remains valid and should not be judged solely through the lens of immediate efficiency. Therefore, public attribution is rather a symbolic gesture with strategic value.

References

[1]. M. Elgan, "A decade of global cyberattacks, and where they left us," IBM, 9 July 2024. [Online]. Available: https://www.ibm.com/think/insights/decade-global-cyberattacks-where-they-left-us. [Accessed 2 September 2025].

[2]. A. Alageel and S. Maffeis, "Investigation of Advanced Persistent Threats Network-based Tactics, Techniques and Procedures," Computer Science, 2025.

[3]. N. Ibrahim, N. Rajalakshmi and K. Hammadeh, "Exploration of Defensive Strategies, Detection Mechanisms, and Response Tactics against Advanced Persistent Threats APTs," Nanotechnology Perceptions, vol. 20, no. 4, pp. 439-455, 2024.

[4]. R. L. Kugler, "Deterrence of cyber attacks," Cyberpower and national security, vol. 320, pp. 309-340, 2009.

[5]. D. Tran, "The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack," Yale JL & Tech, vol. 20, p. 376, 2018.

[6]. A. Schmidt, "The Estonian Cyberattacks," in The fierce domain - conflicts in cyberspace 1986-2012, Washington, D.C., Atlantic Council, 2013.

[7]. F. Nasir and R. Sohail, "State, Surveillance, and Cyberspace: An Intelligence Analysis of Operation Aurora," Social Science Review Archives, vol. 3, no. 2, 2025.

[8]. S. Goel, "How improved attribution in cyber warfare can help de-escalate cyber arms race," Connections , vol. 19, no. 1, pp. 87-95, 2020.

[9]. J. S. Nye, "Deterrence and Dissuasion in Cyberspace," International Security, vol. 41, no. 3, p. 44-71, 2017.

[10]. C. Lu and L. Zhang, "A Chinese Perspective on Public Cyber Attribution," China Quarterly of International Strategic Studies, vol. 8, no. 1, pp. 61-77, 2022.

[11]. N. J. Ryan, "Five Kinds of Cyber Deterrence," Philosophy & Technology, vol. 31, p. 331-338, 2018.

[12]. FBI, "APT 41 GROUP," 3 September 2020. [Online]. Available: https://www.fbi.gov/wanted/cyber/apt-41-group. [Accessed 21 September 2025].

[13]. FBI, "APT 10 GROUP," 7 December 2018. [Online]. Available: https://www.fbi.gov/wanted/cyber/apt-10-group. [Accessed 21 September 2025].

[14]. FBI, "APT 40 CYBER ESPIONAGE ACTIVITIES," 24 November 2020. [Online]. Available: https://www.fbi.gov/wanted/cyber/apt-40-cyber-espionage-activities. [Accessed 21 September 2025].

[15]. F. Egloff and A. Wenger, "Public Attribution of Cyber Incidents," CSS Analyses in Security Policy, vol. 244, 2019.

[16]. J. R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," Journal of Cybersecurity, vol. 1, no. 1, pp. 53-67, 2015.

[17]. F. J. Egloff and M. Smeets, "Publicly attributing cyber attacks: a framework," Journal of Strategic Studies, vol. 46, no. 3, pp. 502-533, 2021.

[18]. European Repository of Cyber Incidents, "Attribution Tracker," [Online]. Available: https://eurepoc.eu/attribution-tracker/. [Accessed 20 September 2025].

[19]. S. Romanosky and B. Boudreaux, "Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government," International Journal of Intelligence and CounterIntelligence, vol. 34, no. 3, pp. 463-493, 2021.

[20]. G. Baram, "Cyber Diplomacy through Official Public Attribution: Paving the Way for Global Norms," International Studies Perspectives, 2024.

[21]. R. Gottemoeller, K. Hedgecock, J. Magula and P. Poast, "Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept," Defence Studies, vol. 22, no. 3, pp. 516-524, 2022.

[22]. M. Grigutytė, "Microsoft Exchange zero-day vulnerability: What do you need to know?," NordVPN, 7 April 2024. [Online]. Available: https://nordvpn.com/blog/microsoft-exchange-exploits/. [Accessed 26 September 2025].

[23]. Microsoft 365 Security; Microsoft Threat Intelligence, "HAFNIUM targeting Exchange Servers with 0-day exploits," 2 March 2021. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/. [Accessed 26 September 2025].

[24]. Foreign, Commonwealth & Development Office; National Cyber Security Centre; The Rt Hon Dominic Raab, "UK and allies hold Chinese state responsible for a pervasive pattern of hacking," 19 July 2021. [Online]. Available: https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking. [Accessed 26 September 2025].

[25]. BBC, "China says Microsoft hacking accusations fabricated by US and allies," 20 July 2021. [Online]. Available: https://www.bbc.com/news/world-asia-china-57898147. [Accessed 26 September 2025].

[26]. Department of Justice, "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians," 25 March 2024. [Online]. Available: https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived. [Accessed 26 September 2025].

[27]. Ministère de l'Europe et des Affaires étrangères, "Russia - Attribution of cyber attacks on France to the Russian military intelligence service (APT28) (April 29th, 2025)," 29 April 2025. [Online]. Available: https://www.diplomatie.gouv.fr/en/country-files/russia/news/2025/article/russia-attribution-of-cyber-attacks-on-france-to-the-russian-military. [Accessed 26 September 2025].

[28]. Secrétariat général de la défense et de la sécurité nationale, "National Strategic Review," 2025. [Online]. Available: https://www.sgdsn.gouv.fr/files/files/Publications/20250713_NP_SGDSN_RNS2025_EN_0.pdf. [Accessed 26 September 2025].

[29]. P. Madhiraju, "France says Russia-backed APT28 hackers targeted Olympic networks and government systems," 1 May 2025. [Online]. Available: https://business-news-today.com/france-says-russia-backed-apt28-hackers-targeted-olympic-networks-and-government-systems/. [Accessed 26 September 2025].

[30]. A. Waldman, "Mandiant upgrades Sandworm to APT44 due to increasing threat," 17 April 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/news/366581178/Mandiant-upgrades-Sandworm-to-APT44-due-to-increasing-threat. [Accessed 26 September 2025].

[31]. Cybersecurity and Infrastructure Security Agency, "New Sandworm Malware Cyclops Blink Replaces VPNFilter," 23 February 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-054a. [Accessed 26 September 2025].