‘What’s in a Name?’: How Does the UK Government and Media Construct Cyber Actors?

Alice Brett and Iain Reid
University of Portsmouth, UK

alice.brett@port.ac.uk
iain.reid@port.ac.uk

Abstract: Understanding how cyber actors are labelled is important to effectively respond to cyber threats. It has been suggested that cyber is becoming increasingly connected to national security concerns, a process called securitisation. This research sought to take a first step towards understanding if securitisation is occurring through examining the evolving conceptualisation of cyber actors in the UK. The research reviewed cybercrime reporting from the UK Government and three UK media websites between 2019-2023, taking a mixed methods approach using thematic analysis to group cyber actors, and content and statistical analysis to detect shifts in these categorisations. The research identified six primary categories used to conceptualise cyber actors: Attackers, Companies, Criminals, White Hats, Hacktivists, and Nation States. The research identified significant changes in multiple subcategories between 2019-2023, influenced by events such as COVID-19, the 2021 Colonial Pipeline ransomware attack, and the changing geopolitical landscape. Notably, there was an increased tendency to associate cyber actors with nation states, particularly evident following the Colonial Pipeline attack which correlated with a shift towards linking cybercrime groups to states, and the 2023 TikTok ban on government devices which saw an increase in companies conceptualised as state influenced. The results also suggested the type of act does not always determine the perception of cyber actors, instead geopolitics appears to have greater influence on conceptualisations. The research additionally found that terms for cyber actors (such as Hackers) are often used loosely and interchangeably. Furthermore, the categories of actors formed a spectrum, especially blurring distinctions between state and criminals. The research recommends organisations consider language around cyber actors more carefully. Further study is recommended to understand if the results found are evidence of securitisation of cyber actors or a consequence of increased state cyber activity.

Keywords: Cybercrime, Securitisation, Fear discourse, Cyber actors

1. Introduction and Background

In Shakespeare’s Romeo and Juliet, Juliet famously asked “What's in a name? That which we call a rose by any other name would smell as sweet”. To contradict Juliet, distinct and well-defined names are important. Varying names for threats can lead to confusion and being unclear on how to respond (Furnell, 2021). In understanding cybercrime an important step is attribution, identifying or naming the actors responsible for specific acts, helping to defend against future incidents by understanding the motivation and tactics of specific actors (DiMaggio, 2022). Attribution is also needed to ensure correct societal responses, yet terms for cyber actors are often used interchangeably (for example, terrorist and criminal) risking disproportionate legal responses (Cap, 2017). Continuing the Shakespeare analogy; not only is a rose being called by multiple names, but other flowers are being called a rose.

When a term or label has no universal definition, it can function as a boundary object; acquiring different meanings across various social groups while maintaining enough commonality for it be used between the groups (Bowker & Star, 2008). One such boundary object is the term National Security, traditionally used in the military context, to defend against an existential threat to the state, it has been expanded to include a wider range of threats (for example, to the economy, environment and society); a process called securitisation (Buzan, Waever and Wilde, 1998). This can set a dangerous precedent as defining something a national security threat legitimises responding with emergency measures, which can take place outside of established political oversight mechanisms (Buzan, Waever and Wilde, 1998). It has been argued there is an increase in the media portraying cyber incidents as a security concern (Boholm, 2021; Zeffiro et al., 2022), with the process of progressively framing cyber issues as an extreme security concern is a known method of securitisation in cyberspace (Hansen & Nissenbaum, 2009).

This paper does not seek to determine if securitisation of cyber actors is occurring in the UK, but to explore if the conceptualisation of cyber actors has shifted, which might be an indication of securitisation. The paper seeks to understand how the UK views cyber actors, if this changed between 2019 to 2023 (a period with a number of events that could be seen as existential threats to the UK) and what factors might have influenced those changes. The paper puts forward a typology for actors, developed from UK perceptions of actors, laying a foundation for further research.

1.1 How are Cyber Actors Viewed?

The predominant portrayal of a cyber actor is of a hacker, often viewed as a lone, young, male, computer genius (Yar and Steinmetz, 2019). The term hacker is often viewed negatively, frequently used interchangeably with criminal and terrorist (Cap, 2017). Sometimes hackers are presented as either *Black Hat* ("bad"), *White Hat* ("good") or *Grey Hat* (somewhere in-between) (Yar and Steinmetz, 2019) whilst allowing for more nuance than only a negative view, it is an oversimplification.

1.2 How are Cyber Actors Categorised?

One of the most common approaches to categorising cyber actors is through a cybersecurity lens. Commercial threat intelligence companies group the Tactics, Techniques and Procedures (TTPs) from incidents into named cyber groups (DiMaggio, 2022). These companies often have their own naming conventions with different attribution frameworks that may not align with each other (Lemay et al., 2018). Additionally, the information used to categorise is often from confidential sources which can create validation issues (Lemay et al., 2018). Grouping actors by TTPs may be useful for clients of specific threat intelligence companies, however doing so creates issues comparing cyber actors between companies and in independently validating the cyber actor groupings.

Another common approach to categorisation in cyberspace is through motivation. Yet motivation can be multifaceted and differ between what society and what actors themselves say the motivation is (Yar and Steinmetz, 2019). Prevalent motivations can also change, Furnell (2021) noted financial and political motivations have become dominant since 2001. Concentrating on motivation also fails to capture the complexity of the actor, such as states undertaking financially motivated attacks (DiMaggio, 2022).

Rather than broad typographies, academic discussion around categorising cyber actors tends to focus on discrete terms. However, within the terms there is disagreement over definitions. For example, for the term Organised Crime there is debate around the extent cybercriminal groups online can be considered "organised" (Lavorgna & Sergi, 2016), and Hacktivism is subjective to the person categorising the activity, deciding if it is hacktivism or terrorism (Yar & Steinmetz, 2019).

Even if there were universally agreed upon terms for cyber actors, it requires an understanding of who performed an incident to be able to apply a term to an act. Attributing cyber incidents is imprecise, with high levels of uncertainty (DiMaggio, 2022). Beyond the technical challenges, the decision to publicly attribute, and framing of cyber actors behind incidents, is a political tool (Egloff, 2022). The state is often attributed a level of responsibility for cyber actors within their jurisdiction (Healey, 2012) and others frame cyber actors in terms of their proximity to the state (Egloff, 2022). This creates the potential for multiple interpretations of cyber actors; who *undertook* the act, and who is *responsible* for the act.

Ultimately, there are multiple perspectives for understanding cyber actors depending on the needs of the person undertaking the typology. More fundamentally, there are challenges in attributing level of responsibility to actors.

2. Methodology

The research applied a mixed methods approach, taking an exploratory sequential design. First, thematic analysis was undertaken to understand the conceptualisation of cyber actors. Quantitative content analysis was then applied to the categories derived from the thematic analysis, to identify if changes had occurred between 2019-2023.

Sources from both government and media were used to capture a range of dialogues. Media reporting was taken from the top three news brands in the UK by engagement; BBC News, Mail Online and The Guardian (Majid, 2023). His Majesty's Government (HMG) reporting was taken from the 'News and Communications' section of the Gov.UK website for the topics 'cyber security', and 'crime, justice and law'. For the latter, as there was no sub-topic for cybercrime, a filter for the specific terms ('cyber', 'computer' or 'online') was applied. Reports were then filtered to remove articles that were not relevant (such as not alluding to a cyber actor in the article).

Reporting was taken from 01 April 2019–31 March 2023, selected to include a timeframe before COVID-19 impacted the UK as it has been observed that some forms of cybercrime have changed since COVID-19 (Wall, 2021). Furthermore, it encompasses multiple geopolitical events which may have influenced the perception of cyber threats, such as the 2022 Russian invasion of Ukraine and heightened tensions in the Indo-Pacific region (Cabinet Office, 2023).

Theoretical thematic analysis, inductively coded for latent themes, was undertaken to develop the categories of cyber actors. The thematic analysis following the six stages put forward by Braun and Clarke (2006). Results from the analysis were used to create categorisations of the cyber actors, with the same data re-analysed using quantitative content analysis. Trend graphs were created from the content analysis to visually identify trends. Specific events were identified through observing spikes in frequency or changes in trends. Articles around these time periods were reviewed for mention of events that may have generated the change.

Table 1: Summary of the six stages of thematic analysis. Edited from Braun and Clarke (2006)

Stage	Description
Data familiarisation	Reading and re-reading, noting initial ideas to gain an in-depth understanding of the data.
Initial code generation	Systematic coding of the data, identifying pertinent features.
Searching for themes	Collation of codes into themes.
Reviewing themes	Refining the themes, checking for internal homogeneity within each theme and external heterogeneity between themes.
Defining and naming themes	Developing analysis for each theme, understanding the 'story' it tells. Generating definitions and names for the themes.
Producing the report	Integrating the analysis with research questions and literature, selecting compelling data extracts.

3. Results

The analysis suggests that HMG and the UK media conceptualise cyber actors in six broad categories: Attackers, Companies, Criminals, White Hats, Hacktivists, and Nation States, with each category having further sub-categories (Table 1). Whilst each category was distinct, categories were frequently associated with each other. For example, in articles with actors categorised as *Nation State-Criminal State*, 32% also mentioned *Nation State-Hacking Groups* and 24% mentioned *Criminals-State Approved*. Likewise, in 20% of the articles referencing *Companies-State Influenced*, *Nation State-Hostile State* were also discussed.

There is a variety of terms used to refer to the same actor, six of the articles reviewed used eight different terms for a single actor within the article. Despite this range of terms, hacker appears as the prevalent term for cyber actors, found in 46% of articles, and used in all categories except for the sub-category of Sexual Perpetrators.

Table 2: Categories of cyber actors

Category	Sub-category	Description
Attackers	Vandals	Individuals or groups who undertake petty or nuisance acts
	Immature	Individuals or groups not understanding the impact of their actions. Usually in reference to teenage boys.
	Personal Malicious	Individuals with personal motivations beyond financial, often with reference to revenge, bullying, or hate crimes.
	Ideological Malicious	Political or ideologically motivated, but not portrayed as activists
	Sexual Perpetrators	Individual sexual perpetrators. Includes judgements about their behaviour being predatory, repulsive, or abusive.
Companies	Mercenary	Private companies acting as mercenaries, providing Nation States with sophisticated cyber tools and/or weapons.
	Amoral	Companies that facilitate criminal activity through inaction or negligence. Often in reference to 'Tech Giants'.
	State Influenced	Companies that are heavily influenced by, or beholden to, a Nation State.
Criminals	State Approved	Organised groups of professional and experienced criminals with links to a Nation State. Often unscrupulous in targeting of their victims.
	Syndicate	Network of criminals that work together. Implies or refers to 'Crime as a Business' and professionalisation.
	Opportunistic Predatory Gangs	Opportunistic and predatory criminal gangs. Able to exploit vulnerabilities in technology or use advanced technology. Unscrupulous and devious, preying on or exploiting victims.

Category	Sub-category	Description
	Sophisticated Gangs	Serious and organised criminal gangs, undertaking sophisticated hacks.
	Cyber Thieves	Individual or multiple people undertaking, usually money or cryptocurrency, heists. Referred to as sophisticated criminal masterminds.
	Lavish Playboys	Individuals showing off their ill-gotten gains. Overt displays of excessive wealth.
	Amateur	Amateur criminals, using unsophisticated techniques or are seen as being incompetent (such as not planning how to evade detection).
	Underground Hackers	Nefarious underground hackers, operating in the shadows. Anonymously operating as individuals or as a community.
White Hats	Ethical Hackers	Hackers working ethically, helping find vulnerabilities for the challenge or the greater good.
	Treasure Hunters	Financially motivated hackers working to help people.
Hacktivists	Vigilantes	Individual activists or vigilantes.
	Political Collectives	Group of hackers working together for a cause.
Nation State	Cyber Warriors	Friendly nations undertaking legal and responsible operations or offensives to hunt the 'bad guys'.
	Hacking Groups	Highly skilled and sophisticated hacking groups directly connected to a nation state.
	Hostile State	Referring to the state itself as an irresponsible and hostile cyber power. Perceived as a national security threat.
	Contracted Hackers	Proxies acting on behalf of a state, contracted or mercenary actors.
	Criminal State	States undertaking crime or using criminal actors to undertake criminal acts.
	Unethical State	States using cyber for perceived unethical reasons, such as hiring mercenary companies to spy on dissidents or spreading general disinformation.

The conceptualisations of cyber actors changed noticeably between 2019-2023 (Figure 1). A brief description of the categories, and significant changes within the larger categories are outlined below.

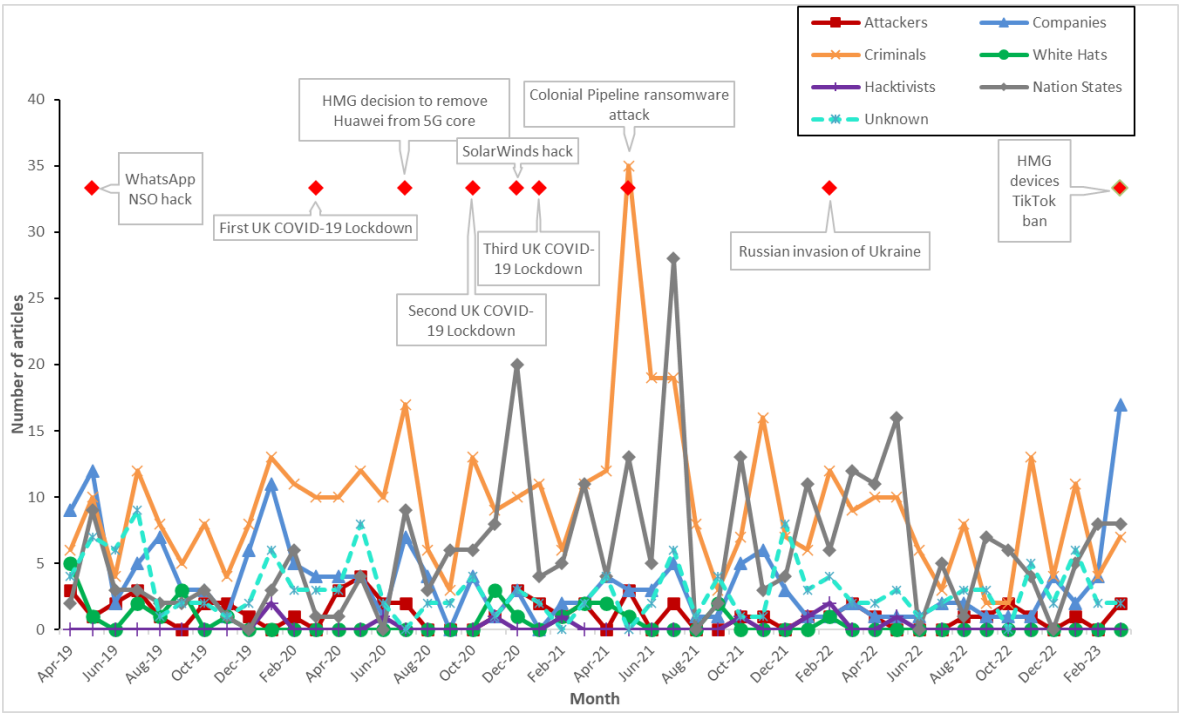

Figure 1: Frequency of articles coded with main categories of cyber actor between April 2019 to March 2023

3.1 Attackers

The Attackers category is predominantly driven by non-financial motives. This category is the most amorphic, more clearly defined by what it is not; they are not financially motivated, nation states, activists, or part of a

collective. Attackers are seen as individual or small groups who are not part of a wider community. They are often referred to by terms such as perpetrator, attacker, or offender, rather than criminal or hacker. Attackers are usually identified as an individual, supplemented with information on their career or education.

3.2 Companies

Companies are seen as being nefarious by the nature of their business (Mercenary), by their actions (Amoral), or that they are unable to be trusted by their provenance (State Influenced). Companies are referred to as an entity in themselves rather than individuals within it. Frequently, articles about companies are accompanied by debates on law and regulation, often looking to tighten rules or introduce new restrictions. Mercenary and State Influenced companies are often seen as proxies for nation states, with most criticism leveraged against the controlling nation. Whereas, for Amoral companies the blame is laid on them, often implying the company was negligent.

All three sub-categories of Companies were found to have significantly changed between 2019-2023. A spike in the portrayal of State Influenced companies correlated with HMG's ban on TikTok (a Chinese company) on its devices. This spike is particularly notable when compared to the similar reporting on HMG's July 2020 decision to remove Huawei (another Chinese company) from the 5G core.

3.3 Criminals

Criminals is the largest category (represented in 46% of the articles), with the actors being construed as criminal. These actors are referred to by multiple terms (for example, hacker, criminals, attackers, fraudsters), with each sub-category having between six (for Amateur) to 33 (State Approved) terms used to refer to actors within it.

Criminal conceptualisations of Generic Group and Sophisticated Gang peaked at the time as the Colonial Pipeline attack, giving rise to State Approved group conceptualisations shortly after. The Colonial Pipeline attack also correlated with changes in how criminal groups are conceptualised, shifting from Generic Groups towards Sophisticated Gangs and State Approved. References to Opportunistic Predatory peaked around the first COVID-19 lockdown but maintained frequent smaller spikes until the summer of 2022 after which its usage declined.

3.4 White Hats and Hacktivists

White Hats and Hacktivists are similar groups, their activities are not seen as criminal (although, this does not mean they are not breaking the law) or as working for a nation state. White Hats are viewed as performing legal hacks to help people (Ethical Hackers) or for financial gain (Treasure Hunters). They are often described as professional and experts, with Ethical Hackers frequently referred to as Security Researchers. Hacktivists are seen as acting unlawfully but with their actions being morally guided, they are not seen as receiving any personal gain. Vigilantes are identified as individuals acting from a perceived injustice, while Political Collectives are closer to the original idea of Hacktivists being political activists and are viewed as a group of hackers acting together for a perceived just cause.

3.5 Nation State

Nation States are viewed as powerful actors in cyberspace, HMG aligns states as being responsible (Cyber Warriors) or irresponsible cyber powers. States are often referred to as being 'prolific' in their hacking and 'sophisticated' in their techniques, performing hacks that civilian companies are unable to defend against. The state is frequently referred separately from the employees (Hacking Groups) or proxies hired (Contracted Hackers) to undertake the hacking. Unethical States are often associated with Companies-Mercenary and are accused of spying on their own people or dissidents living abroad. Criminal States are accused of hacking for monetary gain, often linked with bypassing financial sanctions or passing intellectual property to their own companies. Hostile States are seen as aggressive and enemies of the UK, conducting espionage or destructive attacks, often threatening critical infrastructure.

4. Discussion

The results suggest that there is no clearly defined terminology used to refer to cyber actors, supporting earlier findings that terms are being used interchangeably and indiscriminately (Cap, 2016). Whilst hacker was the prevailing term used; it was still only used in less than half (46%) of the articles. However, the prevalence of the term hacker across multiple categories (found in all sub-categories except Sexual Perpetrator), suggest it has become a boundary object for the categories (Bowker and Star, 2008) having multiple interpretations but retaining the common identity of a cyber actor.

Whilst distinct categories can be seen in the categorisation of cyber actors, there are blurred boundaries between actors. The lack of distinction is especially prevalent where there is a state-criminal nexus or proxy actors. This was seen in the reporting of the Colonial Pipeline attack; Nation State sub-categories of Hacking Group and Contracted Hackers spiked alongside Criminals-State Approved. These categories can be viewed as being on a spectrum of delegation from a state: Hacking Groups directly employed, Contracted Hackers under active direction but with looser ties, and Criminals-State Approved receiving passive sanctioning of their activities. The three categories spiking simultaneously suggests articles conceptualised the attack differently, potentially deciding on different points along the spectrum to report them. This finding may also suggest different conceptualisations of who is *responsible* for the act (i.e. determining state responsibility (Healey, (2012) versus the criminals who undertook the act). Further research is required to determine why these differences in conceptualisation occur.

The type of cyber act perpetrated did not bear directly onto the conceptualisation of the cyber actor. In news reports, for example, ransomware incidents were categorised as being performed by a variety of Criminals and Nation States sub-categories, likewise multiple types of Criminals were accused of fraud or scams. These changes may be reflective of the shifting perceptions of who the cyber actors are that are undertaking different acts, for example the rising tensions with Russia between 2019 to 2023 (Cabinet Office, 2023) may have influenced perceptions of ransomware groups. This suggests TTP based typologies, which focus on technical elements such as the tactics used, may not be useful to understand how we conceptualise threat actors.

Changes in geopolitics impacting the UK (Cabinet Office, 2023) were reflected throughout the articles. Criminals shifted from being referred to as Generic Groups to increasingly labelled as State Approved; for example, in referring to the ransomware group Sodinokibi (also known as REvil) The Guardian referred to the group in January 2020 as simply a "*ransomware gang*" (Jones, 2020) however in June 2021 described them as "*…a flourishing, aggressive group of primarily Russian native speakers based in a former Soviet state and enjoys protection by Russian intelligence or the Russian government*." (Hern & Villarreal, 2021). This changing perception was also evident in the category of Companies. The reporting around the 2023 HMG ban of TikTok on government devices saw almost triple the portrayal of Companies-State Influenced compared with the 2020 ban of Huawei in UK's 5G Core, reflecting the changing language on Chinese influence (Cabinet Office, 2023). Whilst these may be an indication of securitisation, progressively framing events as security concerns (Hansen & Nissenbaum, 2009), it may also be reflective of an increase in nation state cyber activity.

5. Conclusion

To respond to Juliet's question 'What's in a name'; there is a complex interaction between geopolitical events, technological and political considerations with attribution, securitising speech acts, and blurring distinctions in a name. A name is not static. Between 2021-2023, HMG and the UK media constructed cyber actors under six broad categories: Attackers, Companies, Criminals, White Hats, Hacktivists, and Nation States, and presented a changing narrative in their depictions of cyber actors, influenced by events including COVID-19 and the changing geopolitical landscape.

Geopolitics had a strong influence on perceptions of cyber actors in the UK, the articles during key events often blurred the distinctions between state and criminals or companies, which may suggest securitisation is occurring to the conceptualisation of cyber actors, or it may reflect the changing threat landscape. Further research should be undertaken to understand what areas, if any, securitisation has occurred.

The results suggest the common depiction of cyber actors as hackers remains, although multiple terms for cyber actors are used, often loosely and interchangeably. The lack of a common terminology is compounded by reporting using different categorisations of actor for the same event, or for the same actor in different events. Varying names for threats can lead to confusion (Furnell, 2021), and use of ambiguity and terms with negative connotations may cause anxiety (Boholm, 2021). Organisations should decide on specific terms to use for cyber actors and carefully consider connotations with the terms used.

By identifying how the UK views cyber actors this research has provided a typology to categorise and track further changes in reporting on cyber actors. Understanding the changes in representation of cyber actors between 2019 and 2023 indicate a shift in perceptions, laying a foundation for further research to identify why these changing perceptions have occurred.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: AI tools were not used in the creation of this paper

References

Boholm, M. (2021) 'Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019)', *Journal of Cybersecurity*, 7(1), p. tyab016. https://doi.org/10.1093/cybsec/tyab016.

Bowker, G.C. and Star, S.L. (2008) *Sorting things out: classification and its consequences*. 1. paperback ed., 8. print. Cambridge, Mass.: MIT Press (Inside technology).

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. https://doi.org/10.1191/1478088706qp063oa.

Buzan, B., Waever, O. and Wilde, J. de (1998) *Security: a new framework for analysis*. 12. Nachdr. Boulder, Colo.: Lynne Rienner.

Cabinet Office (2023) Integrated Review Refresh 2023: Responding to a more contested and volatile world. https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world

Cap, P. (2017) 'Technological Discourse: Threats in the Cyberspace', in Cap, P., *The Language of Fear*. London: Palgrave Macmillan UK, pp. 53–66. https://doi.org/10.1057/978-1-137-59731-1_5.

DiMaggio, J. (2022) *The art of cyberwarfare: an investigator's guide to espionage, ransomware, and organized cybercrime*. San Francisco: No Starch Press Inc.

Egloff, F.J. (2022) *Semi-state actors in cybersecurity*. New York, NY: Oxford University Press.

Furnell, S. (2021) 'Categorising Cybercrime and Cybercriminals: The Problem and How It Has Changed', *Journal of Information Warfare*, 20(4), pp. 68–76.

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53(4), pp. 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

Healey, J. (2012) 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks', *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/

Lemay, A. *et al.* (2018) 'Survey of publicly available reports on advanced persistent threat actors', *Computers & Security*, 72, pp. 26–59. https://doi.org/10.1016/j.cose.2017.08.005.

Majid, A. (2023). Most popular websites for news in the UK: Monthly top 50 listing. PressGazette. https://pressgazette.co.uk/media-audience-and-business-data/media_metrics/most-popular-websites-news-uk-monthly-2/ (Accessed: 27 June 2023).

Wall, D.S. (2021) 'The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability and the Organisation of Offending', European Law Enforcement Research Bulletin. https://papers.ssrn.com/abstract=3908159

Yar, M. and Steinmetz, K.F. (2019) *Cybercrime and society*. Third edition. Los Angeles London New Delhi Singapore Washington DC Melbourne: Sage.

Zeffiro, A *et al.* (2022) 'Discourses on cybersecurity. The politics of the data breach as a security crisis', *Rivista di Digital Politics*, (3), pp. 369–398. https://doi.org/10.53227/106451.