House of Lords Communications and Digital Select Committee Inquiry
on
Cyber resilience of the UK's Critical National Infrastructure

Written Evidence

Submitted by: ***Dr Akshi Kumar,*** Senior Lecturer in Computer Science, Director-Post Graduate Research (PGR), Department of Computing, Goldsmiths, University of London, United Kingdom

"Guarding the UK's Critical Infrastructure: The Rumour Challenge in Cyber Resilience"

Key Terminology:

- *Rumour:* Rumour is classified as misinformation or disinformation depending on whether it is spread unintentionally or deliberately with deceptive intent.
- *Critical National Infrastructure (CNI)*: CNI refers to vital systems, networks, and assets, both tangible and intangible, that if incapacitated or destroyed would have a debilitating impact on a nation's security, economy, health, or safety. Examples include energy grids, transportation networks, water supply systems, communication infrastructures, and healthcare services.
- *Rumour Control:* This refers to the proactive monitoring, identification, and correction of false or misleading information, especially in the domain of cyber threats or vulnerabilities.

Executive Summary

I. **Rumours and UK's CNI Cyber Resilience:** Rumours can compromise the UK's CNI through tactics like social engineering, phishing campaigns, causing false alarms, public panic, and damaging reputation. Additionally, they can influence political and regulatory outcomes.

II. **Real-world Evidence from Russia-Ukraine Cyber Conflict:** Amid the ongoing Russia-Ukraine conflict, rumours and disinformation campaigns marked by events like the BlackEnergy, NotPetya attacks, and the disinformation campaign of global grain supply, have complicated the understanding of cyber-attacks, highlighting the need for accurate threat intelligence and the danger of misinformation affecting diplomatic and geopolitical relations.

III. **Impact on UK's CNI:** Rumours can disrupt the UK's CNI by inducing public panic, misdirecting resources, compromising operational integrity, and eroding stakeholder trust. Disinformation campaigns might also be used as a tactic by adversaries to mislead or create diversions.

IV. **Future Rumour Landscape:** Over the next two years, the rumour landscape is expected to evolve with more sophisticated tactics, such as deepfakes, AI-generated content, and manipulated media. Emerging platforms and new technologies will offer fresh avenues for rumour dissemination.

V. **Government Cyber Security Strategy 2022-2030:** Government's cybersecurity strategy emphasizes traditional threats; it does not explicitly address the challenges posed by digitally supercharged information space where social media has become a virtual battleground where manipulated information is used as a formidable weapon. While the Online Safety Bill represents a crucial move forward, it alone cannot address the extensive challenges of rumours, especially when a disturbance in one CNI sector can impact others.

VI. **Enhancing CNI Cyber Resilience:** To strengthen the UK's CNI cyber resilience against rumours, it's essential to integrate international best practices, understand the extensive impact of rumours on CNI, and employ innovative models for proactive and reactive strategies. The integration of AI and the Susceptible-Infected-Recovered-Anti-spreader (SIRA) model in healthcare CNI offers transformative information control with implications for all critical infrastructures.

Question 1. How do rumours potentially compromise the security and operation of CNI?

1. **Social Engineering Attacks[1]:** Rumours can be used to manipulate individuals within an organization, including those responsible for CNI, into taking actions that compromise security. For example, spreading false information about an impending security threat could lead to unnecessary shutdowns or disruptions in critical infrastructure.

2. **Phishing and Spear Phishing:** Cybercriminals often use rumours to craft convincing phishing emails or messages to trick employees into clicking on malicious links or downloading malware[2,3]. This can lead to breaches of CNI systems.

3. **False Alarms:** Rumours about security incidents can trigger false alarms and emergency responses[4]. Responding to non-existent threats can strain resources and divert attention from real threats, potentially leaving CNI vulnerable.

4. **Public Panic:** Rumours that reaches the public can lead to panic and overreactions, such as hoarding resources[5] or fleeing urban areas. This can indirectly impact CNI by disrupting supply chains and causing logistical challenges[6,7].

5. **Reputation Damage:** If rumours about a CNI organization is spread, it can harm its reputation and public trust. This can lead to a loss of confidence from stakeholders, including investors and customers, which may impact the organization's ability to operate effectively[8].

Question 2. How have rumours and disinformation campaigns influenced the perception and response to cyber-attacks during the Russia-Ukraine conflict, and what implications does this have for geopolitical relations and cyber diplomacy?

The Russia-Ukraine conflict, which began with Russia's annexation of Crimea in 2014, has witnessed a number of cyber-attacks on both sides. The cyber domain became a notable battleground, and rumours and disinformation campaigns surrounding these cyber activities became rife. In fact,

---

[1]Advanced social engineering attacks
https://doi.org/10.1016/j.jisa.2014.09.005
[2] Coronavirus Social Engineering Attacks: Issues and Recommendations
https://pdfs.semanticscholar.org/3abf/fa2b63727dbcee307493fca1004e58bebfd6.pdf
[3] Large Language Models Can Be Used To Effectively Scale Spear Phishing Campaigns
https://arxiv.org/abs/2305.06972
[4] Social media amplification loops and false alarms: Towards a Sociotechnical understanding of misinformation during emergencies
https://www.tandfonline.com/doi/full/10.1080/10714421.2022.2035165
[5] Is it really "panic buying"? Public perceptions and experiences of extra buying at the onset of the COVID-19 pandemic
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0264618
[6] The Use of Cyberwarfare in Influence Operations
https://en-cyber.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf
[7] Influence operations and the modern information environment
https://scholar.archive.org/work/42ctlgafwbgzndbvc33vemc4vu/access/wayback/https://www.bloomsburycollections.com/book/hybrid-warfare-security-and-asymmetric-conflict-in-international-relations/ch8-influence-operations-and-the-modern-information-environment.pdf?dl.
[8]The relationship between cyber-attacks and dynamics of company stock: the role of reputation management
https://www.inderscienceonline.com/doi/abs/10.1504/IJESDF.2022.123891

manipulating social feeds with false accounts, bots, targeted ads and other methods can be considered a type of cyberattack[9]. Below are some instances and the implications of these rumours:

6. BlackEnergy Malware & Ukrainian Power Grid (2015)[10]

6.1. ***Event:*** In December 2015, a significant portion of Ukraine's power grid was disrupted by a cyber-attack. The malware, known as BlackEnergy, was identified as the culprit.

6.2. ***Rumour and Reality:*** There were immediate rumours and speculations about the origin of the attack, with many pointing fingers at Russian state-sponsored actors. While circumstantial evidence pointed in that direction, definitive attribution took time, and the rumours added layers of confusion.

6.3. ***Implication:*** This situation underscored the importance of accurate threat intelligence and attribution. Rumours can impact diplomatic relations and might lead to hasty policy decisions.

7. NotPetya Ransomware Attack (2017)[11]

7.1. ***Event:*** In June 2017, a destructive malware, later named NotPetya, spread rapidly across the world but primarily affected Ukrainian businesses.

7.2. ***Rumour and Reality:*** Initial beliefs were that this was just another ransomware meant to extort money. However, it soon became clear that the malware was wiper malware masquerading as ransomware, leading to rumours about its potential political motivations and origins. It was later attributed with high confidence to Russian military hackers by several western governments.

7.3. ***Implication:*** The rumours and subsequent truth about NotPetya's origins increased global tensions and led to a re-evaluation of how nation-state cyber-attacks might be conducted under the guise of criminal activity.

8. Russia's War on Ukraine's Grain and Global Food Supply (2023) [12,13,14]

8.1. ***Event:*** On July 17, 2023, Russia exited the Black Sea Grain Initiative (BSGI), leading to a 17% rise in global grain prices and announcing their record exports, exploiting market vulnerabilities amid disinformation campaigns and increased aggression towards Ukraine.

---

[9] Cyberattack Misinformation Could Be Plan for Ukraine Invasion
https://www.scientificamerican.com/article/cyberattack-misinformation-could-be-plan-for-ukraine-invasion/
[10] When The Lights Went Out
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
[11] Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down
https://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/
[12] Disinformation and Russia's war of aggression against UkraineThreats and governance responses
https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/
[13] Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges
https://www.mdpi.com/2078-2489/14/9/485
[14] Russia's War on Ukraine's Grain and Global Food Supply, in Five Myths
https://www.state.gov/russias-war-on-ukraines-grain-and-global-food-supply-in-five-myths/

8.2. ***Rumour and Reality:*** In the aftermath of Moscow's withdrawal from BSGI, the Kremlin continued to distort data, deny facts, and manipulate math attempting to perpetuate five false myths. The Kremlin falsely depicts Russia as a sanction's victim and downplayed Ukraine's global grain relevance, while Moscow misrepresented its role in global food security and intensified attacks on Ukraine's ports, undermining both Ukraine's economy and global grain distribution. But the hard truth is that despite disinformation, sanctions didn't restrict Russia's grain. Ukraine's grain remains vital for global food supply, yet Russian aggression jeopardizes its exports and price stability.

8.3. ***Implication:*** Russia's disinformation campaign threatens Ukraine's exports and global price equilibrium. The implications extend far beyond the immediate and apparent economic impact towards a deeper geopolitical and strategic ambitions[15]. They underscore the intricate link between geopolitics, economics, and food security in today's interconnected world.

9. The Russia-Ukraine conflict serves as a stark reminder of the role of rumours in shaping the cyber landscape during geopolitical tensions. The spread of false or unverified information can exacerbate tensions, lead to misguided policy decisions, and strain international relations. It underscores the need for rigorous verification and rumour control in cyber operations during conflict scenarios.

Question 3. How do rumours impact the cyber resilience of the UK's CNI?

The challenge of rumours in the cyber resilience of the UK's CNI is not just relevant but crucial.

10. Public Panic and Misinformation: In the age of rapid information dissemination through social media and other online platforms, rumours can spread quickly. A rumour about a failure or breach in a critical infrastructure can cause unnecessary public panic[16]. The chaos ensuing from such misinformation can exacerbate an already critical situation[17].

11. Misdirection of Resources[18],[19]: Responding to false alarms or rumours can divert valuable resources from actual threats or issues. This can delay responses to real incidents, potentially causing more damage.

12. Operational Integrity: CNI sectors depend on accurate information for operations. If decision-makers receive and act on misinformation, it can lead to wrong decisions that disrupt the smooth functioning of infrastructure services[20].

---

[15] Russia Expands Its War on Ukraine — to Global Food Supplies
https://www.usip.org/publications/2023/07/russia-expands-its-war-ukraine-global-food-supplies

[16] Crime In The Time Of The Plague: Fake News Pandemic And The Challenges To Law-Enforcement And Intelligence Community
https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_14746_sr_2020_4_2_10

[17] The Landscape of Disinformation on Health Crisis Communication During the COVID-19 Pandemic in Ukraine: Hybrid Warfare Tactics, Fake Media News and Review of Evidence
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8425291/

[18] Time for Action A report exploring the impact of false alarms in Wales
https://www.gov.wales/sites/default/files/publications/2019-06/time-for-action.pdf

[19] Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9994786/

13. **Disinformation as a Tactic:** Adversaries might use disinformation campaigns deliberately[21]. By spreading false information about a cyber-attack or a vulnerability, they can create a diversion while launching a real attack elsewhere[22],[23]. Alternatively, they might exaggerate the impact of an actual attack to create a perception of a more severe breach, sowing further chaos. Further, state-sponsored actors might use rumours as a part of influence operations aimed at weakening public confidence in a country's CNI or creating divisions between allies. Over time, this can weaken a nation's ability to respond to real cyber threats.[24]

14. **Stakeholder Trust:** Trust is paramount when it comes to CNI. If stakeholders (which include the general public, regulatory bodies, and government entities) can't rely on the authenticity of information from CNI entities due to prevalent rumours, it erodes trust, making effective communication and cooperation difficult[25].

15. **Impact on Economy[26]:** Rumours about vulnerabilities or breaches in critical sectors, like banking, can lead to significant economic repercussions. For instance, a rumour about a bank's insolvency (even if untrue) can trigger a panic-driven withdrawal by its customers. Similarly, rumours related to the financial stability or integrity of CNI entities, like power companies or water treatment facilities, can lead to fluctuations in their stock prices or even broader economic consequences if investors and markets believe the rumours.[27]

Question 4: How will rumour landscape develop over the next two years?

Predicting the exact trajectory of the rumour landscape over the next two years is challenging due to the dynamic and evolving nature of information dissemination. However, we can make some informed assessments based on current trends and factors. Here are some potential developments:

16. **Increased Sophistication:** Rumour tactics are likely to become more sophisticated, with a growing use of deepfakes, AI-generated content, and manipulated media. Detection and debunking will also need to evolve to keep up.

---

[20] Detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions
https://link.springer.com/article/10.1007/s10479-022-05015-5
[21]Information warfare, disinformation and electoral fraud
https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html
[22] Combined cyber and physical attacks on the maritime transportation system
https://par.nsf.gov/biblio/10166239
[23] Security analysis of drones systems: Attacks, limitations, and recommendations
https://doi.org/10.1016/j.iot.2020.100218
[24] Digital doomsday: The threat of cyber attack hangs over all of us, but how big could it get? Could hackers bring society to a standstill — a digital Armageddon?
https://ieeexplore.ieee.org/abstract/document/9246763
[25] Strategic Cyber Security Management
https://api.pageplace.de/preview/DT0400.9781000636338_A43165719/preview-9781000636338_A43165719.pdf
[26]The Cost of Malicious Cyber Activity to the U.S. Economy
https://www.hsdl.org/?view&did=808776
[27] Economic Effects Of The Fake News On Companies And The Need Of New Pr Strategies
https://www.ceeol.com/search/article-detail?id=714176

16.1. ***Deepfakes***[28]***:*** Deepfakes are hyper-realistic, AI-generated videos, audio recordings, or images that manipulate and superimpose individuals' likenesses onto fabricated content. These have gained notoriety for their potential to deceive viewers into believing fabricated scenarios or statements. Expectations include:

a) *Greater Realism:* Deepfakes are expected to become even more convincing, making it increasingly challenging to discern real from fake content.

b) *Diverse Applications:* Beyond political or celebrity impersonations, deepfakes may be used in various contexts, including corporate impersonations, fraud, or even personal vendettas.

16.2. ***AI-Generated Content:*** Artificial intelligence tools can generate written content using large language models (LLMs), including news articles, blog posts, and social media comments. AI-generated text can mimic human writing styles and may be used to create fake news or propaganda[29],[30]:

a) *Content Volume:* There may be a surge in AI-generated content, flooding the internet with misleading or false information.

b) *Customization:* AI-generated content can be tailored to specific audiences or contexts, increasing its potential impact. Moreover, automated bots using AI-generated content can flood social media platforms with misleading comments, amplifying particular viewpoints or causing confusion.

16.3. ***Manipulated Media:*** Visual and audio media, including photos, videos, and audio recordings, can be manipulated using advanced software[31]. This includes simple edits to create misleading narratives or more complex manipulations:

a) *Subtle Manipulations:* Manipulated media can be used to subtly alter the context or details of real events, making them appear different from reality, altering the public's understanding of the situation.

b) *Hybrid Content:* Expect an increase in the creation of hybrid content that combines elements of real and manipulated media, further complicating detection.

17. *Evolving Platforms and Channels:* The platforms and channels through which misinformation spreads will continue to change. Social media platforms, messaging apps, and emerging technologies may become prominent vectors for rumours.

17.1. ***Social Media Platforms:*** Social media platforms have been instrumental in the rapid dissemination of rumours in the UK. As the landscape evolves:

a) *Diverse Platforms:* Beyond major platforms like Facebook and Twitter, smaller or niche social media platforms may emerge as new vectors for spreading rumours[32].

---

[28] Deepfakes, misinformation and disinformation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism
https://doi.org/10.1177/14648849211060644

[29] All the News That's Fit to Fabricate: AI-Generated Text as a Tool of Media Misinformation
https://doi.org/10.1017/XPS.2020.37

[30] Synthetic Lies: Understanding AI-Generated Misinformation and Evaluating Algorithmic and Human Solutions
https://doi.org/10.1145/3544548.3581318

[31] Visual Mis/disinformation in Journalism and Public Communications: Current Verification Practices, Challenges, and Future Opportunities
https://doi.org/10.1080/17512786.2020.1832139

[32] Between alternative and traditional social platforms: the case of gab in exploring the narratives on the pandemic and vaccines
10.3389/fsoc.2023.1143263

b) *Algorithmic Amplification:* Social media algorithms can unintentionally amplify sensational or misleading content, potentially leading to the viral spread of rumours[33].

17.2. ***Messaging Apps:*** Private messaging apps, such as WhatsApp and Telegram, have gained popularity in the UK and pose unique challenges:

a) *Encrypted Communication:* End-to-end encryption in messaging apps can make it challenging for authorities to monitor or counteract rumours shared within closed groups[34].

b) *Rapid Dissemination:* Rumours can spread swiftly within private groups, making it difficult to detect and address before it reaches a broader audience[35].

18. ***Emerging Technologies:*** The adoption of emerging technologies introduces new avenues for misinformation:

a) *AI-Driven Dissemination:* AI-powered bots and automated systems can target UK audiences on various platforms, spreading rumours at scale[36],[37].

b) *Virtual Reality (VR) and Augmented Reality (AR):* As VR and AR technologies become more accessible, there may be potential for rumours to be disseminated in immersive and convincing ways[38].

Question 4. How adequately does the Government Cyber Security Strategy 2022-2030 adequately address the concept of rumour as a cyber threat?

19. The government's current cybersecurity strategy, spanning from 2022 to 2030, articulates a vision for enhancing the nation's resilience to cyber threats[39]. The strategy sets forth a central aim: to significantly harden government's critical functions against cyberattacks by the year 2025, with the ultimate goal of ensuring that all government organizations across the entire public sector are resilient to known vulnerabilities and attack methods no later than 2030.

20. The strategy's central aim reflects a clear commitment to bolstering the cybersecurity posture of government entities, safeguarding critical infrastructure, and ensuring the uninterrupted delivery of essential services. The pursuit of this aim entails a comprehensive approach encompassing technology, policy, and workforce development, among other aspects.

21. While this strategy is laudable in its ambition and commitment to enhancing the overall cybersecurity resilience of the government, it is crucial to recognize that the strategy primarily focuses on traditional cybersecurity challenges, such as protecting critical infrastructure, securing

---

[33] The impact of social media algorithms on content distribution
https://aicontentfy.com/en/blog/impact-of-social-media-algorithms-on-content-distribution
[34] Messaging Apps: A Rising Tool for Informational Autocrats
https://doi.org/10.1177/1065912923119093
[35] Hidden Virality and the Everyday Burden of Correcting WhatsApp Mis- and Disinformation
https://www.ideals.illinois.edu/items/126256
[36] Tool of the War-A Three-Minute Animated Futuristic Film About AI-Powered Fake News and Disinformation
https://www.proquest.com/openview/e538d439c16126a20a2173243792b286/1?pq-origsite=gscholar&cbl=18750&diss=y
[37] Exploring Ethical Implications of ChatGPT and Other AI Chatbots and Regulation of Disinformation Propagation
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4461801
[38] The Future of Social Media
https://cbscreening.co.uk/news/post/the-future-of-social-media/
[39]Government Cyber Security Strategy Building a cyber resilient public sector
https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

data, and responding to cyber threats. As of its current formulation, the strategy does not explicitly incorporate measures tailored to addressing the specific challenges posed by rumour-related threats.

22. Online Safety Bill[40] is a crucial step in regulating the online space and protecting users from online harms, it's not sufficient on its own to address the comprehensive cyber resilience needs and threats faced by the UK's CNI. A combination of multiple legislative measures, technical solutions, public-private partnerships, sharing of information & threat assessments between IT departments and industrial security teams[41] and international cooperation is essential to guard the UK's critical infrastructure comprehensively.

Question 5. How do different nations approach the challenge of rumours and misinformation in safeguarding their CNI's cyber resilience?

23. Nations worldwide acknowledge the impact of rumours on the cyber resilience of their CNI. While approaches vary, most combine regulation, technological solutions, public awareness campaigns, and international collaboration to tackle this multifaceted challenge. Here are two examples:

24. United States:

24.1. ***Department of Homeland Security (DHS)[42]:*** The DHS has a dedicated Cybersecurity and Infrastructure Security Agency (CISA) to manage risks to critical infrastructure. CISA regularly releases alerts and advisories, including those related to disinformation.

24.2. ***Partnership with Private Sector:*** The U.S. collaborates with tech companies in Silicon Valley to curb the spread of misinformation, especially during elections, when infrastructure like voting machines is vulnerable[43].

24.3. ***Public Awareness Campaigns:*** CISA has launched campaigns such as "War on Pineapple" to educate the public about disinformation tactics using light-hearted, relatable content[44],[45].

25. Germany:

25.1. ***Federal Office for Information Security (BSI)[46]:*** This body oversees IT security for the nation, including guarding against rumours and misinformation affecting critical sectors.

---

[40] A guide to the Online Safety Bill
https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill

[41] Cyber Risk Framework for Critical Infrastructure Threat Scenario: Mapping the Consequences of an Interconnected Digital Economy
https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf

[42] Cybersecurity and Infrastructure Security Agency (CISA)
https://www.dhs.gov/keywords/cybersecurity-and-infrastructure-security-agency-cisa

[43] Big Tech Companies Meeting With U.S. Officials on 2020 Election Security
https://www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html

[44] THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps
https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf

[45] U.S. cybersecurity agency uses pineapple pizza to demonstrate vulnerability to foreign influence
https://www.nbcnews.com/news/us-news/u-s-cybersecurity-agency-uses-pineapple-pizza-demonstrate-vulnerability-foreign-n1035296

[46] Federal Office for Information Security: BSI
https://www.bsi.bund.de/EN/Home/home_node.html

25.2. ***NetzDG Law:*** While its primary focus is hate speech, this law obligates large online platforms to remove "obviously illegal" content within 24 hours, indirectly addressing misinformation[47],[48].

25.3. ***Collaboration with EU:*** As a key EU member, Germany takes part in the EU's initiatives against disinformation and cooperates with its Rapid Alert System[49].

26. For UK, understanding various international strategies and mechanisms can provide a well-rounded perspective. While every country has unique challenges based on its socio-political environment, cultural context, and historical events, best practices from these nations can be adapted and integrated into a comprehensive strategy for guarding the UK's critical infrastructure against rumours in the realm of cyber resilience.

27. The relevance of rumour control becomes even more pronounced given the potential domino effect a disruption in one area of CNI can have on others[50]. Undeniably, CNI's protection from misinformation threats is paramount to national security, public trust, and the smooth functioning of essential services.

28. Understanding the universality of rumour mechanics is crucial, irrespective of the sector. For instance, the healthcare-focused Susceptible-Infected-Recovered-Anti-spreader (SIRA) model[51] provides an innovative framework, considering both entities that propagate rumours and those that aim to control them. Utilizing the principles of the SIRA model, we can derive or modify a CNI-specific framework. This would simulate potential rumour scenarios and their subsequent control, guiding proactive and reactive strategies within CNI sectors. Embracing advanced models and tools, exemplified by the SIRA approach, is paramount for predicting and thwarting rumour propagation within CNI. This paves the way for fortified CNI cyber resilience, safeguarding national interests.

Question 6. How can the convergence of AI and the SIRA model in healthcare be adapted and scaled across various sectors of CNI to address sector-specific challenges and enhance overall security, predictability, and public trust?

29. The convergence of AI and the SIRA model in healthcare social networks marks a transformative step in information control, with potential implications extending well beyond the healthcare sector. This integration holds far-reaching consequences for the entirety of critical national infrastructures.

---

[47] Germany's balancing act: Fighting online hate while protecting free speech
https://www.politico.eu/article/germany-hate-speech-internet-netzdg-controversial-legislation/
[48]Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform
https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf
[49]Factsheet: Rapid Alert System
https://www.eeas.europa.eu/node/59644_en
[50] Countering disinformation with facts - Russian invasion of Ukraine
https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng
[51] SIRA: a model for propagation and rumor control with epidemic spreading and immunization for healthcare 5.0
https://doi.org/10.1007/s00500-022-07397-x

29.1. **Predictive Capabilities Across Sectors:** Just as AI and the SIRA model can foresee and mitigate the spread of health-related rumours, similar models can be designed to predict threats or vulnerabilities in other sectors of CNI. For instance, in the energy sector, predictive analytics could anticipate potential failures or breaches, thereby ensuring continuous power supply.

29.2. **Enhanced Security Protocols:** Misinformation can be as damaging in sectors like finance and transportation as it is in healthcare. By integrating AI-driven models akin to SIRA, these sectors can devise stronger and more adaptive security protocols, reducing the risk of security breaches resulting from misinformation or manipulated data.

29.3. **Real-time Response Systems:** In sectors like telecommunications, a real-time response system to threats can prevent large-scale outages or disruptions. The union of AI and models like SIRA can facilitate instant threat detection and reaction mechanisms.

29.4. **Improved Public Trust:** As observed in healthcare, dispelling myths and providing accurate information boosts public trust. Other CNI sectors, like water supply or public transportation, can benefit from such trust. Implementing AI-driven models ensures that misinformation is kept at bay, thus maintaining public confidence.

29.5. **Inter-sectoral Collaboration:** AI and SIRA's successful collaboration in healthcare can be a model for other CNI sectors to foster inter-sectoral collaborations. For instance, the transportation and energy sectors can work together using AI to optimize energy use in public transport systems.

29.6. **Standardized Framework:** The introduction of such advanced models can lead to the development of a standardized framework for information control and security across all CNI sectors. This ensures uniformity in response mechanisms, regardless of the specific challenges each sector faces.

29.7. **Knowledge Sharing and Continuous Learning:** Successes and challenges in applying AI and the SIRA model in healthcare can serve as lessons for other sectors. Such cross-industry knowledge sharing can foster innovation and ensure that best practices are adopted universally.

30. In essence, the integration of AI and the SIRA model in healthcare CNI isn't just a sector-specific advancement; it's a harbinger of a more interconnected, secure, and resilient future for all critical infrastructures.

31. There are essential policy implications to consider:

31.1. ***Regulatory Oversight:***

a) *Need:* Given the potential harm of healthcare rumours, there may be a need for platforms, especially those related to health, to adopt and implement the SIRA model or similar methodologies.

b) *Implementation:* Governments could mandate certain platforms, especially those with significant influence in healthcare spaces, to integrate such models. Regular audits can ensure compliance and effectiveness.

31.2. ***Collaboration:***

a) *Need:* Tech platforms alone might not always have the expertise to discern medical misinformation. Collaboration with health organizations can bridge this knowledge gap.

b) *Implementation:* Formal partnerships can be established between tech companies and healthcare organizations. These entities can work together to validate information, devise strategies to counter misinformation, and even co-create content to educate the public.

31.3. ***Public Education:*** Public awareness campaigns about the dangers of healthcare rumours and the importance of verified information.

a) *Need:* A well-informed public is the first line of defence against the spread of health-related rumours. By understanding the sources of reliable information and the dangers of unverified claims, individuals can make better healthcare decisions and prevent the spread of false narratives.

b) Implementation:

i. Awareness Initiatives: Launch public campaigns underscoring the perils of healthcare-related rumours and emphasizing the significance of authenticated sources.

ii. Knowledge Dissemination: Spearhead public drives that highlight the risks associated with health misinformation while advocating for reliance on verified data.

iii. Educational Campaigns: Organize outreach programs that caution against the pitfalls of unverified healthcare claims and stress the value of accurate, validated knowledge.

iv. Collaborative Workshops: Engage healthcare professionals, tech platforms, and community leaders to host informational workshops at schools, colleges, and community centres.

v. Engage Influencers: Partner with prominent figures in society, from celebrities to online influencers, to champion the cause of accurate health information dissemination.

vi. Community Enlightenment: Roll out initiatives that educate the masses about the detrimental impact of healthcare myths and underscore the importance of turning to trustworthy sources.

vii. Informational Outreach: Implement broad-based educational efforts to alert the public about the hazards of health-related rumours and champion the need for well-validated information.

32. For 'Guarding the UK's Critical Infrastructure: The Rumour Challenge in Cyber Resilience', the integration of AI with the SIRA model in healthcare social networks emerges as a beacon of innovation. This convergence not only showcases a cutting-edge approach to managing healthcare information but also serves as a blueprint for strengthening cyber resilience. By countering misinformation and strengthening defence, it underscores the necessity to safeguard the entirety of the UK's critical national infrastructures from potential threats.

x----------x

Credentials and the foundation for the evidence submission concerning the cyber resilience of the UK's CNI

Greetings,

I am Dr. Akshi Kumar, a distinguished researcher and academic in the fields of Natural Language Processing (NLP), social media analysis, and network modelling. With years of dedicated research and comprehensive studies, in my previous and current organizations, at both individual level and with international collaborators, I have cultivated a unique expertise in understanding digital behaviour, misinformation dynamics, and network vulnerabilities – aspects critically intersecting with the cyber dimensions of national infrastructures worldwide.

Our organization, working collaboratively with a diverse network of researchers and experts, has persistently ventured into the complexities of digital misinformation, network vulnerabilities, and the propagation mechanisms in our digital age. The depth and breadth of our investigations are evidenced by the following published works:

i. Kumar, S., **Kumar, A.,** Mallik, A., Singh, R.R. (2023) *"OptNet-Fake: Fake News Detection in Socio-cyber platforms using Grasshopper Optimization and Deep Neural Network"* IEEE Transactions on Computational Social Systems- https://doi.org/ 10.1109/TCSS.2023.3246479
ii. **Kumar, A.,** Kumar, S.*, Aggarwal, N. (2022). *"SIRA: A Model for Propagation and Rumor Control with Epidemic Spreading and Immunization for Healthcare 5.0"*, Soft Computing, A Fusion of Foundations, Methodologies and Applications, Springer, https://doi.org/10.1007/s00500-022-07397-x
iii. Kumar, S., **Kumar, A**. *, Panda B.S. (2022) *"Identifying Influential Nodes for Smart Enterprises using Community structure with Integrated Feature Ranking"* IEEE Transactions on Industrial Informatics, https://doi.org/10.1109/TII.2022.3203059
iv. Kumar, S., **Kumar, A**. *, Mallik, A., Dhall, S. (2022) *"Opinion Leader Detection in Asian Social Networks using Modified Spider Monkey Optimization"* ACM Transactions on Asian and Low-Resource Language Information Processing (ACM TALLIP), https://doi.org/10.1145/3555311
v. Jain, DK, **Kumar, A**.*, Shrivastava, A. (2022). *"CanarDeep: A Hybrid Deep Neural Model with Mixed Fusion for Rumour Detection in Social Data Streams",* Neural Computing and Applications, Springer 10.1007/s00521-021-06743-8
vi. **Kumar, A.,** Bhatia MPS, Sangwan, SR*. (2021). *"Rumour Detection using Deep Learning and Filter-Wrapper Feature Selection in Benchmark Twitter dataset",* Multimedia Tools and Applications,
vii. **Kumar A.,** Sangwan S R, Nayyar A (2019). *"Rumour Veracity Detection on Twitter using Particle Swarm Optimized Shallow Classifiers"*. Multimedia Tools and Applications, 10.1007/s11042-019-7398-6
viii. **Kumar, A.,** Singh, V., Ali, T., Singh, J. (2020). *"Empirical Evaluation of Shallow and Deep Architecture Classifiers on Rumour Detection",* In Advances in Computing and Intelligent Systems, Springer.
ix. **Kumar, A.,** Sharma, H. (2020). *"PROD: A Potential Rumour Origin Detection Model using Supervised Machine Learning,"* In International Conference on Intelligent Computing and Smart Communication 2019, Springer.
x. **Kumar, A.** & Sangwan, S R. (2018). *"Information Virality Prediction using Emotion Quotient of Tweets",* International Journal of Computer Sciences and Engineering, https://doi.org/10.26438/ijcse/v6i6.642651.

xi. **Kumar, A.,** Sangwan, SR. (2018). *"Rumour Detection using Machine Learning Techniques on Social Media",* International Conference on Innovative Computing and Communication, Lecture Notes in Networks and Systems, Springer

The crucial importance of the UK's CNI to our nation's functional and operational capacities is a well-established fact. With the digital age unfolding more complexities, it becomes imperative that experts from diversified domains collaborate, sharing insights and strategies to develop a robust and resilient cyber infrastructure.

The driving force behind my submission of evidence on this subject is twofold:

a) *Evolving Threat Landscape:* The convenience and progress ushered in by the digital age come accompanied by sophisticated threats. Misinformation, digital behavioural manipulations, and inherent network vulnerabilities can critically compromise our CNI with repercussions on national security, the economy, and societal well-being.

b) *The Imperative of Collaborative Defence:* Cyber resilience demands a concerted effort. It's a mosaic of contributions from network analysts, NLP experts, behavioural scientists, and infrastructure specialists. Our organization, fortified by its extensive research and global collaborations, stands ready to provide invaluable insights and innovative measures to enhance the UK's CNI's resilience against potential cyber threats.

In conclusion, my overarching goal is to harness my expertise and research findings in fortifying the UK's CNI cyber resilience. Through combined efforts, knowledge-sharing, and sustained dialogue, we can work towards a more secure and robust digital future for the UK.

Warm regards,
Akshi

Dr. Akshi Kumar (*She/Her)*
Senior Lecturer (Associate Professor)-Computer Science,
Director of Post-Graduate Research (PGR),
Member of Research Ethics Committee,
Department of Computing,
Goldsmiths, University of London
New Cross, London SE14 6NW

Endorsed by *Royal Academy of Engineering*, UK: Exceptional promise in the field of AI/Data Science, 2022
"Top 2% scientist of the world", Stanford University List, USA in 2022 and 2021
Member, Turing Natural Language Processing Interest Group, UK
Member, British Computer Society (BCS) and ACM
Senior Member, IEEE