Understanding public reactions to cybersecurity incidents

Miguel Alberto Gomez | Center for Security Studies, ETH Zurich | @mgomez85

Theme

Against the widespread belief that public opinion is likely to panic in response to severe cybersecurity incidents, the relevant scholarship is putting this belief and the associated narratives into question. This analysis offers a brief overview of how public opinion approaches and responds to cybersecurity incidents.

Summary

It is fair to say that our understanding of how public opinion reacts to an incident in cyberspace has progressed significantly in the past few years. Contrary to previous assumptions, in which uncertainty and fear lead to a public reaction somewhere between panic and paralysis in the aftermath of cybersecurity incidents, current research points to an increased public knowledge about the limited societal or physical impacts of disruptive incidents. A greater knowledge undermines the narratives of securitisation that exaggerate the impact of incidents in the daily life of ordinary people. A better understanding of public reactions would help cybersecurity authorities to improve their communication and deterrence procedures about severe incidents.

Analysis

Transcending panic and paralysis

Cybersecurity incidents that disrupt essential services or potentially contribute to the loss of life continue to reinforce narratives of the existential threat posed by malicious behaviour in and through this human-made space.[1] Popular culture and high-profile incidents in recent years do little to curb the apparent validity of such claims. As observed by Jarvis, Macdonald & Whiting,[2] these narratives frequently surface in the news despite limited evidence to support claims of wide-ranging damage following such cybersecurity incidents.

These depictions hinge on the idea that public opinion is inherently sensitive and likely to panic in response to severe cybersecurity incidents. As convincing as this argument may be, the public's comprehension and response to cybersecurity incidents remains under-explored. More often than not, the argument that increases the societal

[1] The recent incidents involving the Colonial Pipeline and University of Dusseldorf Hospital ransomware typifies this phenomenon.

[2] L. Jarvis, S. Macdonald & A. Whiting (2017), 'Unpacking cyberterrorism discourse: specificity, status, and scale in news media constructions of threat', *European Journal of International Security*, vol. 2, nr 1, p. 64-87.

dependence on these technologies is likely to invoke anxiety and dread among the public that malicious actors might exploit is readily accepted. Consequently, this leads some to assert the strategic potential of cyber operations.[3]

However, cybersecurity scholarship in the past five years leads us to question the validity and expected outcomes of these narratives. Instead of simply being anxious and passive, cyber-dependent public opinion exhibits a fair degree of nuance in how it responds to cybersecurity incidents. Although the public exhibits a degree of apprehension concerning malicious behaviour, a fair amount of agency is observed in terms of its perception and reaction. This paper offers a brief overview of how the public approaches and responds to cybersecurity incidents. Specifically, it reveals findings established through experimental research that integrate insights from political science, psychology and sociology to better understand public behaviour and opinion.

To guide readers, the remainder of this paper is organised into three sections. Following the introduction, it presents an overview of commonly held assumptions following cybersecurity incidents. This lays the groundwork necessary to identify the appeal of recurring narratives, which is then followed by presenting findings in contemporary cybersecurity scholarship that depict public opinion as an engaged actor that uses: (1) emotions; (2) knowledge; and (3) individual experience to form preferences and opinions. Finally, the paper closes with a brief discussion of how these developments influence the development of cybersecurity policy.

Pervasive assumptions

The depiction of public opinion following severe cybersecurity incidents often portrays it as panic-stricken and disempowered in the face of society-wide effects. Although popular media exaggerate such reactions for entertainment, there remains a grain of truth in these scenes. The potential for exaggerated reactions to severe cybersecurity incidents is rooted in: (1) the uncertainty of the environment; and (2) the rarity of severe cybersecurity incidents.

Cyberspace is a fundamentally uncertain environment owing to the underlying technology and interconnectivity that enables it. Uncertainty, in this case, refers to the ambiguity of the information rather than the lack of it.[4] Information Communication Technologies (ICT), that constitute the basic component of cyberspace, are frequently characterised as being inherently vulnerable. For instance, an estimated 15 to 50 flaws are expected for every 1,000 lines of code.[5] While not all of them are likely to result in catastrophic failure, complexity makes it difficult to predict precisely where and how

[3] R.A. Clarke & R.K. Knake (2014), *Cyber War*, Tantor Media Inc., Old Saybrook.

[4] B.C. Rathbun (2007), 'Uncertain about uncertainty: understanding the multiple meanings of a crucial concept in international relations theory', *International Studies Quarterly*, vol. 51, nr 3, p. 533-557.

[5] Dan Mayer (2012), 'Ratio of bugs per line of code', *Continuously Deployed* (blog), 6/XII/2012, https://www.mayerdan.com/ruby/2012/11/11/bugs-per-line-of-code-ratio.

failure will occur.[6] These technologies build on one another for cyberspace to function and are selected primarily on the grounds of interoperability rather than security.[7]

Early cybersecurity scholarship cites dependence on this uncertain environment as a factor for the hypersecuritisation of cyberspace.[8] Current trends in ICT usage across societies lend credence to the argument that cyberspace's unknowable and unpredictable nature leads to uncertainty concerning the consequences following the exploitation of vulnerable technologies. [9] On this premise, early cybersecurity commentators argued for the devastating effects of malicious behaviour on cyberspace.[10] This narrative is further encouraged by journalistic representations of the outcome of severe cybersecurity incidents that highlight the possible impact on critical infrastructure and other cyber-dependent services.[11] However, this begs the question of how common these incidents are.

Malicious behaviour in cyberspace that results in physical or societal effects is rare. The Dyadic Cyber Incident and Dispute Dataset (DICD),[12] for instance, only identifies 29 such campaigns carried out by six actors as having succeeded in meeting their objectives. This is approximately 10% of all cyber campaigns listed in the dataset. Considering the opaque nature of these activities, it is likely that the actual proportion is much lower. In addition, these activities require significant material and organisational resources that effectively limit the number of actors capable of carrying them out.[13] Finally, capable actors may not want to engage in such activities for the sake of doing so. As noted by Maness & Valeriano,[14] a fair amount of restraint exists among cyber-capable actors that reflects the need to avoid unwanted escalation, especially in cases where malicious behaviour in cyberspace coincides with other salient disputes.

One would expect that the rarity of severe cybersecurity incidents would temper anxiety among the public. Paradoxically, however, the rarity of these incidents tends to result in misperception among the public should they occur. Research on responses and

[6] C. Perrow (2011), *Normal Accidents: Living with High Risk Technologies – Updated Edition*, Princeton University Press.

[7] J.R. Lindsay (2017), 'Restrained by design: the political economy of cybersecurity', *Digital Policy, Regulation and Governance*.

[8] L. Hansen & H. Nissenbaum (2009), 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, vol. 53, nr 4, p. 1155-1175.

[9] M. Dunn Cavelty (2013), 'From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse', *International Studies Review*, vol. 15, nr 1, p. 105-122.

[10] I. Saltzman (2013), 'Cyber posturing and the offense-defense balance', *Contemporary Security Policy*, vol. 34, nr 1, p. 40-63.

[11] Jarvis, Macdonald & Whiting (2017).

[12] B. Valeriano & R.C. Maness (2014), 'The dynamics of cyber conflict between rival antagonists, 2001-11', *Journal of Peace Research*, vol. 51, nr 3, p. 347-360.

[13] J.R. Lindsay (2013), 'Stuxnet and the limits of cyber warfare', *Security Studies*, vol. 22, nr 3, p. 365-404; E.D. Borghard & S.W. Lonergan (2017), 'The logic of coercion in cyberspace', *Security Studies*, vol. 26, nr 3, p. 452-481; R. Slayton (2016), 'What is the cyber offense-defense balance? Conceptions, causes, and assessment', *International Security*, vol. 41, nr 3, p. 72-109.

[14] R.C. Maness & B. Valeriano (2016), 'The impact of cyber conflict on international interactions', *Armed Forces & Society*, vol. 42, nr 2, p. 301-323.

assessments[15] note that risks that are unknowable and uncontrollable are worrying even when they are statistically rare. Relatedly, the absence of personal experience with these incidents results in a pronounced response. Even if domain experts agree with one another about the likelihood of such events, public perceptions are likely to remain misaligned due to their lack of experience.

Taken collectively, the uncertainty resulting from domain characteristics coupled with fear and sustained media exposure without first-hand experience results in the misalignment between the actual likelihood of these events and public perception. Consequently, this further empowers narratives that emphasise the existential threat posed by severe cybersecurity incidents that, in turn, shape public perceptions.

Observations of public behaviour

While the idealised approach to understanding how the public responds to cybersecurity incidents is to observe behaviour following such an event, doing so consistently and rigorously is problematic given the nature of this phenomenon. However, recent experimental studies that utilise hypothetical cybersecurity incidents offer valuable insight that challenges commonly held notions surrounding the publics' reactions to these events. Broadly, these studies note that: (1) anxiety is not pervasive vis-à-vis cyberspace; (2) it is not the sole emotion facilitating public behaviour; and (3) public opinion is not passive following a severe cybersecurity incident.

Although the narratives surrounding public reactions to cyberspace encouraged by popular culture often depict panic and anxiety following a severe cybersecurity incident, little to no empirical evidence offers support. For instance, Gomez & Whyte [16] demonstrate that while repeated exposure to cybersecurity incidents causes an increase in negative emotions, it does not appear to be pronounced. Informing individuals of adverse events in cyberspace, on its own, did not appear to lead to elevated levels of concern relative to those who were informed of neutral events (i.e., the acquisition of one IT company by another). In addition, neither domain knowledge nor trust in cyberspace appear to explain the observed outcome.

[15] C.F. Camerer & H. Kunreuther (1989), 'Decision processes for low probability events: policy implications', *Journal of policy analysis and management*, vol. 8, nr 4, p. 565-592; G. Gigerenzer (2006), 'Out of the frying pan into the fire: Behavioral reactions to terrorist attacks', *Risk Analysis: An International Journal*, vol. 26, nr 2, p. 347-351; G.Y. Reinhardt (2017), 'Imagining worse than reality: comparing beliefs and intentions between disaster evacuees and survey respondents', *Journal of Risk Research*, vol. 20, nr 2, p. 169-194.

[16] M.A. Gomez & C. Whyte (2021), 'Breaking the myth of cyber doom: securitization and normalization of novel threats', *International Studies Quarterly*.

These observations stand in stark contrast with proposed explanations for public reactions following severe cybersecurity incidents. Instead, the authors argue that a process of threat normalisation accounts for these observations. That is to say, constant exposure to these technologies, over time, results in the acceptance of the risks associated with engaging in cyberspace. This risk-literature supports[17] the argument as individuals appear to be more risk-acceptant when participating in activities in which the associated risk is known ahead of time. In other words, individuals are offered a degree of control in terms of their decision to participate or not.

However, these findings do not conclusively answer whether the public's reaction to cybersecurity incidents is exclusively a function of anxiety. Although the study mentioned above points to negative emotions surfacing following incidents, this does not delineate whether this refers primarily to anxiety, anger or fear. Identifying which of these emotions are at work is crucial as these have distinct effects on cognitive processes. For instance, anxiety tends to encourage greater introspection and increases the tendency for risk minimisation.[18] In contrast, anger is an action-oriented emotion encouraging individuals to take action.[19]

In a series of experiments, researchers at the University of Haifa[20] identify anger as the dominant emotion following severe cybersecurity incidents. During these experiments, participants are shown fictitious videos of news reports detailing malicious behaviour in cyberspace targeting critical infrastructure that result in the loss of life. In these cases, anger surfaces as the emotion that influences public preferences. Interestingly, this finding is comparable to instances where the damage to critical infrastructure resulted from a terrorist rather than from a cyber-attack.

In the study, higher levels of anger translated into significant public support for retaliation –possibly increasing the risk of escalation if involving a state actor–. This process, in which individual emotions experienced at the personal level translate into support for polity-wide policies is supported by findings from Gomez & Whyte,[21] that show that threats to the polity are evaluated at the level of the individual. In other words, the self is used as the reference point as to what may threaten the wider society. This mechanism runs counter to how the public is depicted as panicking following severe cybersecurity incidents. Instead, these events may trigger greater militancy on the part of 'victims' and may contribute to increased tension and destabilisation.

[17] Loran F. Nordgren, Joop Van Der Pligt & Frenk Van Harreveld (2007), 'Unpacking perceived control in risk perception: the mediating role of anticipated regret', *Journal of Behavioral Decision Making*, vol. 20, nr 5, p. 533-544.

[18] J.S. Lerner & D. Keltner (2001), 'Fear, anger, and risk', *Journal of personality and social psychology*, vol. 81, nr 1, p. 146.

[19] A.H. Fischer & I.J. Roseman (2007), 'Beat them or ban them: the characteristics and social functions of anger and contempt', *Journal of personality and social psychology*, vol. 93, nr 1, p. 103; E. Halperin, A.G. Russell, C.S. Dweck & J.J. Gross (2011), 'Anger, hatred, and the quest for peace: anger can be constructive in the absence of hatred', *Journal of Conflict Resolution*, vol. 55, nr 2, p. 274-291.

[20] M.L. Gross, D. Canetti & D.R. Vashdi (2017), 'Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes', *Journal of Cybersecurity*, vol. 3, nr 1, p 49-58; R. Shandler, M.L. Gross, S. Backhaus & D. Canetti (2021), 'Cyber terrorism and public support for retaliation – a multi-country survey experiment', *British Journal of Political Science*, p. 1-19.

[21] Gomez & Whyte (2021).

Fortunately, this is not a foregone conclusion. Scholars such as Kreps & Schneider,[22] for instance, observe that the US public recognises cyberspace as being normatively distinct from the conventional domains of land, sea and air. This distinction appears to encourage greater restraint when extending support for retaliatory action. Similarly, Shandler, Gross & Canetti[23] add more nuance to their earlier findings when they established that support for retaliation is predicated on knowledge of the potential consequences of these actions. In other words, support for retaliation wanes when the public is informed of the negative consequences of this course of action.

While research on how the public responds to malicious behaviour in cyberspace still represents a small subset of cybersecurity scholarship, initial findings appear to question our understanding of public behaviour and preferences. Rather than being passive and anxious recipients of consequences, the public have likely come to accept the risk associated with the integration of cyberspace as part of their daily lives. As disruptive as these may be, the exploitation of cyber-dependent systems does not result in a pronounced sense of alarm as frequently depicted. However, when such events rise to these levels, the public is not passive and is likely to demand an active response.

Conclusions

Implications for policy

Since becoming an issue of national security, elites continue to shape the narrative surrounding threats to and from cyberspace.[24] Consequently, this suggests that public perceptions of cyberspace are in line with how policymakers perceive this human-made environment. This paper and the considerations above call this into question.

With more evidence surfacing that public opinion has distinct views concerning the state of cyberspace, especially in terms of threats, policymakers need to re-assess the extent to which the narratives they espouse resonate among their constituents. For instance, support for improved cybersecurity practices may fail to deliver results if public opinion normalises the risks involved in cyberspace. Conversely, policymakers should also consider the pressure that public opinion might exert on them following the disclosure of severe cybersecurity incidents. While the decision to go public may function to deter future threats,[25] doing so might provoke the public to call for a more forceful response depending on the incident's consequences. This leaves political leaders in the difficult situation of effectively deterring potential adversaries without risking an escalation while balancing domestic concerns and courting the displeasure of the public.

[22] S. Kreps & J. Schneider (2019), 'Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics', *Journal of Cybersecurity*, vol. 5, nr 1, tyz007.

[23] R. Shandler, M.L Gross & D. Canetti (2021), 'A fragile public preference for cyber strikes: evidence from survey experiments in the United States, United Kingdom, and Israel', *Contemporary Security Policy*, p. 1-28.

[24] S. Lawson & M.K. Middleton (2019), 'Cyber Pearl Harbor: analogy, fear, and the framing of cyber security threats in the United States, 1991-2016', *First Monday*.

[25] F.J. Egloff & M. Smeets (2021), 'Publicly attributing cyber attacks: a framework', *Journal of Strategic Studies*, vol. 1, nr 32.

It is fair to say that our understanding of how public opinion reacts to an incident in cyberspace has progressed significantly over the past 20 years. Rather than being passive and anxious, public opinion appears to have accepted the realities of operating in an increasingly cyber-dependent global society. However, acceptance is not passive, and agency is exercised if malicious behaviour crosses a particular threshold. Recognising this dynamic is crucial as it calls for a critical assessment of cybersecurity policies thus far.