Journal of Strategic Competition — Vol. 2, No. 1, 2026

Encouraging Whistleblowing Among Generational Cybercriminals Facilitating Governmental Cyberespionage

Tim Pappa[1] and Olga Kuprina[2]

Abstract

Cybercriminals supporting governmental intelligence and military espionage who are encouraged to become whistleblowers could singularly disrupt the global and geopolitical order. This practitioner's position paper suggests that encouraging cybercriminals to become whistleblowers by demonstrating real and imagined peer whistleblowing of corruption and abuse could provide some balance, as many nations become more transparent even when forced because they lack information on what negative or questionable information will be revealed. There are changing generational norms suggesting that younger generations in different countries are more willing to vocalize allegations or evidence of fraud and corruption within their organizations, which is much more consistent with whistleblowing behaviors found in literature. This exploratory practitioner's position paper integrates research on the changing generational whistleblowing norms and models of shame and guilt influencing behavior in different cultures, proposing a conceptual behavioral paradigm and narrative model suggesting how cybercriminals could be motivated or encouraged to become whistleblowers. We suggest that whistleblowing could continue to emerge as a naturalizing act that diffuses undemocratic and adversarial postures of international political and military decision-makers. This paper will visualize the application of this proposed narrative conceptual model to two theoretical scenarios where there is corruption and abuse uncovered in governmental cyberespionage.

Keywords: cyberespionage, whistleblowing, cybercrime, narrative persuasion, shame, guilt

1 Supervisory special agent (former), Behavioral Analysis Unit (BAU), Federal Bureau of Investigation (FBI).

2 Former offensive cyber operations practitioner, senior threat intelligence analyst, behavioral and forensic linguistics fesearcher focused on generational dynamics in Slavic-language Cyber threat ecosystems.

Introduction

This practitioner's position paper attempts to reimagine the narratives of (cyber)criminal whistleblowers and how cybercriminals might be motivated to disclose information to the public. Collier and Hutchings[3] have sobered many of the characterizations of cybercrime in their writing on the "social ecology" of cybercrime.

The reality of this ecology is that many of these so-called communities on dark web forums and markets are, in fact, populated by minimally skilled people, performing limited functions that contribute to much larger enterprises of cybercrime, perhaps like a ransomware or fraud affiliate. Few people occupy roles such as malware developers for major ransomware gangs.

We are approaching this practitioner's position paper from perhaps interdependent perspectives – the first author is a former agent and profiler with the Federal Bureau of Investigation's Behavioral Analysis Unit (BAU) who specialized in communication strategies targeting cybercriminals, and the second author is a former cybercriminal felon who has conducted cyberespionage campaigns on behalf of governments while active with a cybercriminal gang. We are agnostic in this paper, recognizing these scenarios could also include cybercriminals operating as informants for American intelligence and law enforcement agencies that accept information or request information derived from cyberespionage activity.

Based on our own experience, we concur with Collier and Hutchings' characterization of the individuals who predominantly populate criminal dark web forums and marketplaces. However, we also emphasize that a subset of these actors (by virtue of their specialized access and roles) could exert disproportionate influence, depending on the client and the target, particularly if their cybercrime or cyberespionage activities were exposed to the public as part of documented wrongdoing or fraud. Certainly, we are not advocating any kind of increase in cybercrime or cyberespionage, but we are suggesting that the people in this "ecology" of cybercrime are uniquely positioned to disrupt governments and publics around the world, if they chose to disclose information that would benefit the public because that information revealed corruption or something much worse by a government against people, such as genocide.

From this position of understanding the range of cybercriminals' motivations and life experiences, we want to highlight the real possibilities of a cybercriminal making decisions that benefit the public, even while engaged in cybercrime or cyberespionage.

Chen referred to Gundlach et al. (2003) who established a social information processing model based on prior prosocial organizational behavior paradigms, that suggested people make whistleblowing decisions based on "interpreting misconduct and information of actors."[4] Gundlach et al. defined the steps in this process as observing fraudulent or harmful behavior, making an attribution to that behavior or finding someone responsible for that behavior and making a decision about their own responsibility in reporting that

3 Ben Collier and Alice Hutchings, 2023, "Cybercrime: a social ecology," *The Oxford Handbook of Criminology*, p. 13.

4 Qtd. in Li Chen, 2019, "A review of research on whistle-blowing," *American Journal of Industrial and Business Management*, vol. 9, no. 2, p. 4, https://doi.org/10.4236/ajibm.2019.92019.

behavior. The final step is reporting that behavior. We suggest that this social information processing model applies to the same kind of process a cybercriminal may experience when making a similar decision.

Ceva and Bocchiola[5] have consistently defined whistleblowing by elements of practice, where there is someone within an organization who voluntarily reports some wrongdoing allegedly occurring within that organization, with the desire to stop or correct that wrongdoing or fraud. Snowden in this definition was a whistleblower, but Ceva and Bocchiola considered WikiLeaks founder Julian Assange a "false positive" or not a whistleblower because he does not fit many of their requirements, namely that he is positioned outside the organizations where a whistleblower has disclosed information. Within this characterization, Ceva and Bocchiola considered defining those elements important to avoid "conceptual inflation" of whistleblowing and people associated with whistleblowing or simply other forms of disclosure.

Colvin wrote that the phenomenon of whistleblowing on state crimes is often misunderstood, stating that these "truthtellers" are instead "placed into the archaic frame of crimes against the state or contemporary anxieties about cybercriminality."[6] Colvin suggested whistleblowers in this context should also be recognized as human rights "defenders."[7]

As an example, Colvin considered Snowden's whistleblowing to be a demonstration of how the "disclosure of information can generate accountability and concrete change".[8] Some of that change has included the introduction and passage of new surveillance laws in other countries as well as an emerging market for communications privacy and safe communications. Colvin wrote that Snowden's revelations show "exactly why disclosure is such a powerful tool for tackling state crimes. It is hard to imagine another means of achieving results on a comparable scale or at such range."[9] Colvin suggested there may be greater support for even anonymous disclosure, citing several recent whistle-blowing campaigns in Europe that encouraged anonymized information that could be verified related to alleged antitrust violations, as an example. Colvin highlighted historical examples as well that have perhaps been characterized in more criminal contexts, but which are arguably also disruptive acts of "truthtellers" trying to disclose so-called "state crimes," such as the Citizens' Commission to Investigate the FBI that broke into a smaller FBI office in Pennsylvania in approximately 1971, revealing COINTELPRO documents later used in Congressional investigations of domestic surveillance and other alleged abuses by the FBI.

Many of these examples can be disruptive to attempts by governments to control information. Colvin noted that "disclosures of state crimes are highly disruptive to this discursive power."[10] Colvin differentiated whistleblowing from espionage, writing that espionage is concerned with "establishing or maintaining a differential information advantage

5 Emanuela Ceva and Michele Bocchiola, 2019, "Theories of whistleblowing," *Philosophy Compass*, vol. 15, no. 1, https://doi.org/10.1111/phc3.12642.
6 Naomi Colvin, 2018, "Whistle-blowing as a form of digital resistance: State crimes and crimes against the state, *State Crime Journal*, vol. 7, pp. 26-7, https://doi.org/10.13169/statecrime.7.1.0024.
7 Colvin, 2018, pp. 26-7.
8 Colvin, 2018, pp. 30-1.
9 Colvin, 2018, p. 31.
10 Colvin, 2018, p. 29.

for a select group", while whistleblowing is generally defined as disclosing information for the public good and accountability. Colvin concluded that the public should decide if the information from any source is beneficial and if those "truthtellers'" actions are justified.

Generally, the scale of access to or knowledge of sensitive information of a cybercriminal supporting governmental cyberespionage efforts if shared publicly could abruptly reestablish geopolitical norms overnight and disrupt nation state disinformation efforts. The contemporary norms of cyberespionage suggest that espionage is generally not considered an act of war, therefore whistleblowers who appear to be acting independently could be considered, theoretically, to be an agnostic geopolitical role player in a world where leaking has precedent. But what if this happened?

Gannon et al. wrote about how "capable actors" could arguably engage in "shadow deterrence" because there could be a "broader repertoire of possible actions" in this gray zone.[11] The American government encouraging a cybercriminal committing cyber espionage for a foreign government to disclose evidence of wrongdoing, such as genocide committed by that foreign government, would likely prompt responsive declarations and demonstrations of force. The American government discretely facilitating that whistleblowing could be just as effective. Gannon et al. a couple years before had suggested the need to "act more furtively"[12] because of existing deterrence networks and perhaps what has been characterized as "ritualization of deterrence" demonstrated by governments and militaries in a range of domains.[13] Gannon et al. added that how someone responds to deterrence is more important than whether they are deterred or not. Deterrence is less about preventing and more about changing the nature of those engagements or anticipated engagements. This kind of unorthodox approach would be disruptive, but it could arguably encourage the same approach by foreign governments interested in maligning the American government. There is already demonstration of this approach to espionage to expose real or imagined reputationally damaging information about an adversary government or adversary political leader in both foreign and domestic environments. We are suggesting there is greater motivation and benefit for the public if these kinds of cybercriminals reveal evidence of wrongdoing or fraud that could save lives, for example.

Malksoo wrote that there is a vulnerability among governments that have an illusion of control. Additionally, the same author contended that there are reflections of that illusion in rational deterrence theory and deterrence strategy as an international relations conflict management practice.

Malksoo explained that these repeated "chains of deterrence interactions" or deterrence rituals can create not only norms but social bonds among governments in alliance. Enabling a cybercriminal supporting a foreign government committing cyber espionage who

11 J. Andres Gannon, Erik Gartzke, Jon Lindsay, and Peter Schram, 2024, "The shadow of deterrence: Why capable actors engage in contests short of war," *Journal of Conflict Resolution*, vol. 68, nos. 2-3), p. 11, https://doi.org/10.1177/00220027231166345.

12 J. Andreas Gannon, Erik Gartzke, Jon Lindsay, and Peter Schram, 2020, *After Deterrence: Explaining Conflict Short of War*, https://peterschram.com/wp-content/uploads/2020/12/$12_0 1_2 020_a fter_d eterrence2.pdf$.

13 Maria Malksoo, 2021, "A ritual approach to deterrence: I am, therefore I deter," *European Journal of International Relations*, vol. 27, no. 1, p. 54, https://doi.org/10.1177/1354066120966039.

is willing to disclose publicly information related to fraud and wrongdoing that could influence change in that foreign government and those foreign people reminded us of chaos. We explored chaos theory as a possible framework for examining the possible impact of a government encouraging whistleblowing on another government by enabling or facilitating these cybercriminals involved in cyber espionage.[14] Chaos theory is "concerned with the existence of unpredictable, non-linear relationships and complex elements" of systems. We believe this definition fits the kind of whistleblowing we are encouraging.

We are speculating, but we believe this kind of chaotic "blended approach" could be managed in a state-based irregular strategy to complement broader deterrence.[15] Ucko and Marks noted this distinguishing feature of this approach as they characterized when citing the 2018 National Defense Strategy that highlighted how Russia was effective in Ukraine initially because it used "corruption, predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change facts on the ground."[16]

Ucko and Marks wrote that this exploitation of an adversary government's "social and political contradictions" can delegitimize them and help the American government in this example to gain leverage.[17]

There are norms of governmental cyberespionage, but what about norms for cybercriminals conducting cyberespionage?

Libicki questioned how cyber espionage was considered at that point in time to be acceptable state behavior, while cyber attacks were not.[18] His work on the "coming of cyber espionage norms" explored how governmental responses to different forms of cyberattacks—and the ways in which stolen information was subsequently used—began to normalize certain forms of cyber espionage. The most normalized context of cyber attack appeared to be that cyber espionage is mutually acceptable "as long as the results are used in a 'professional manner'", meaning military and intelligence agencies retain data or other information pursuant to their national security platforms but they do not sell or share that stolen data to commercial or cybercriminal enterprises. Additionally, Libicki included sharing that data with the public as unacceptable, but we note that even these norms are mercurial given the right kind of deniable operation or leak. Libicki summarized his paper as a suggestion of a normative framework that characterizes cyberespionage as unacceptable unless the results of that cyberespionage are used "only to inform national-security

14 Levent Altinary and Metin Kozak, 2021. "Revisiting destination competitiveness through chaos theory: The butterfly competitiveness model," *Journal of Hospitality and Tourism Management*, vol. 49, p. 3, https://doi.org/10.1016/j.jhtm.2021.10.004.

15 Eugenio Lilli, 2021, "Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence," *Contemporary Security Policy*, vol. 42, no. 2, https://doi.org/10.1080/13523260.2021.1882812.

16 David Ucko and Thomas Marks, 2022, *Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action*, p. 21.

17 Ucko and Marks, 2022, pp. 22-3.

18 Martin Libicki, 2017, "The coming of cyber espionage norms," in *2017 9th International Conference on Cyber Conflict (CyCon)*, IEEE, p. 9.

decision-making".

Libicki wrote about brandishing cyberattack capabilities to influence these norms, describing examples where the government warns of cyberattacks targeting local and state networks in efforts to compromise electoral systems, but in the process may also undermine trust in those systems as the attackers or a foreign government may have intended.[19] Libicki characterized the past several years as a "rocky road" to cyberespionage norms,[20] but he highlighted how there are other norms that could be transgressed, such as how attacks or targeting of critical infrastructure are responded to and what happens when the United States vocalizes attribution or warnings to suspected governments of attacks. There are increasingly established norms against cyberespionage for the economic gain of the attacking government, but there are still challenges to what could be characterized as doxing or whistleblowing depending on how the victim of that information disclosure appears to be. Libicki wrote that Moscow could argue that organizations they consider to be anti-Russian including the World Anti-Doping Agency could have been influenced or driven to reveal the whistleblowing that alleged that many Russian athletes were using illegal substances to enhance their performance.[21] Another example might be the Yemen Cyber Army's disclosure of Saudi Arabian Ministry of Foreign Affairs documents they obtained or stole that were then shared with WikiLeaks, which Libicki wrote "might be applauded in some quarters".[22]

While in some of these cases, the disclosure of these kinds of allegations could include documents or data that could perhaps be verified, Libicki concluded again that the norms of cyberespionage among governments continue to be considered acceptable "as long as" that theft is kept within intelligence and military domains. Libicki was concentrating on norms among governments, however, not norms among cybercriminal collectives and gangs, for example. Those examples continue to become much more diffuse. One of the authors previously featured a case study of a futurist model of a fugitive trans hacker merchandiser, and how that hacktivist made meaning from the merchandise she created from her hacking experiences. American law enforcement officials indicted this Swiss trans hacktivist in March 2021 for over a dozen hacks where she publicly disclosed proprietary information from more than a hundred organizations. Officials noted the profit from "hacking-inspired clothing" she created as an overt act in her criminal conspiracy. There are growing examples of hacktivists like this fugitive trans hacker who proclaim a range of motivations and identities that reflect increasingly diffuse hack-and-leak narratives across cybercrime communities.

This paper suggests there are plausible scenarios in which a government may encourage the disclosure of a foreign cybercriminal's cyberespionage on behalf of another state if it benefits that government's national security objectives. This unorthodox approach could fit into Finnemore's and Sikkink's "life cycle of norms" conceptual framework.[23] Finnemore

19 Martin Libicki, 2021, *Cyberspace in peace and war*, Naval Institute Press.
20 Libicki, 2021, p. 143.
21 Libicki, p. 2021, pp. 168-9.
22 Libicki, 2021, p. 170.
23 Martha Finnemore and Kathryn Sikkink, 1998, "International norm dynamics and political change," *International organization*, vol. 52, no. 4, pp. 895-8, https://doi.org/10.1162/002081898550789.

and Sikkink wrote about how "norm building" can emerge from many different origins when promoted by "norm entrepreneurs"[24] and organizational platforms for those entrepreneurs or advocates,[25] to demonstrate those norms or the impact of those norms. The practice of recruiting confidential informants to provide information is a norm among law enforcement and intelligence communities in most countries but making that norm more public in an appeal to cybercriminals involved in cyber espionage to share their information on wrongdoing would require "norm building."[26] The other end of the spectrum in this example could be governmental programs like the U.S. Department of State's Rewards for Justice program, designed to provide monetary rewards in exchange for information on wanted terrorists and nation state attackers. That approach to offering rewards for information is also a confidential norm that has developed. Finnemore and Hollis explored the construction of norms for global cybersecurity using the same framework.[27] Finnemore and Hollis argued that some of the projects on defining norms in cybersecurity have conceptualized norms as "products"[28] focused on saying something instead of detailing and demonstrating how that norm would work in different environments. Finnemore and Hollis wrote that norm cultivation does not work that way:

> Norms are social creatures that grow out of specific contexts via social processes and interactions among particular groups of actors... the real power of norms... lies in the processes by which they form and evolve. The success of a norm rests not just in what it says, but in who accepts it, not to mention where, when, and how they do so.[29]

Finnemore and Hollis emphasized that norm cultivation "culminates when the content of the norm becomes, well, normal – when the norm becomes so taken-for-granted that actors simply assume it as a social fact and part of 'the way things are done'."[30] Researchers exploring the application of this framework within international organizations like the United Nations have both praised and criticized this framework, but there is agreement that the framework recognizes that "norm entrepreneurs" may be nations and nations that singularly act when they want to.[31] Finnemore and Hollis have also highlighted the influence of culture in norm building and norm demonstration. This paper presumes the hesitancy of American governmental institutions leading norm change as proposed in this paper because that so-called norm could be demonstrated against American military and intelligence communities. There is a cultural foundation to American institutions encouraging democratic change and development even if that includes whistleblowing, but there is likely fear that the communities of adversaries working against American government

24 Finnemore and Sikkink, 1998, p. 893.
25 Finnemore and Sikkink, 1998, pp. 895-8.
26 Finnemore and Sikkink, 1998, p. 896.
27 M. Finnemore and D.B. Hollis, 2016, "Constructing norms for global cybersecurity," *American Journal of International Law*, vol. 110, no. 3, https://doi.org/10.1017/S0002930000016894.
28 Finnemore and Hollis, 2016, p. 453.
29 Finnemore and Hollis, 2016, p. 427.
30 Finnemore and Hollis, 2016, p. 453.
31 Finnemore and Hollis, 2016, p. 456.

interests would encourage this whistleblowing of what they might define as fraud and wrongdoing or what may be actual fraud.

The changing generational nature of whistleblowing in Russia and China

Whistleblowing is a complex phenomenon that must be grounded in not only ethnic and organizational cultures, but especially in the context of someone's life.

People with different lived experiences may have different concepts of what is ethical or moral. Cheng, Karim and Lin conducted an empirical examination of cultural influences on whistleblowing decisions and the perceptions of whistleblowing from generally collectivist and individualistic cultures. The results suggested that people from collectivist cultures were generally less likely to become whistleblowers, although this study was based on British and Chinese students at a Scottish university who were presented with whistleblowing scenarios. While they recognized there are many personal factors influencing someone's decision to become a whistleblower, their study suggested that one of the more important factors was the cultural practice and acceptance or non-acceptance of whistleblowing. As an example, they referred to Zhuang et al. who found that collectivist cultures or environments can drive more reporting of wrongdoing.[32] Zhuang et al.'s study revealed that Chinese people had a higher tendency than Canadians to report questionable behavior or peers, suggesting that the desire to protect the collective reputation of a group or organization may have motivated more reporting from Chinese participants than Canadian participants.

While Americans may be more likely to report major and minor fraud, younger generational Chinese are increasingly more likely to report fraud or wrongdoing.[33] We continue to find more recent research that reveals or suggests generational and gender nuances[34] beyond some of this comparative general commentary on collectivistic or individualistic cultures.[35] James, Colemean, and Li referred to surveyed Chinese millennials in the past decade who report being more individualistic and materialistic than older generations.[36] Some of these studies also suggested that Chinese millennials feel less loyal to their employers and more likely to consider leaving their employer than older employees they work with.

32 Julia Zhang, Randy Chiu, and Liqun Wei, 2009, "Decision-making process of internal whistleblowing behavior in China: Empirical evidence and implications," *Journal of Business Ethics*, vol. 88, https://doi.org/10.1007/s10551-008-9831-z.

33 John Keenan, 2007, "Comparing Chinese and American managers on whistleblowing," *Employee Responsibilities and Rights Journal*, vol. 19, no. 2, https://doi.org/10.1007/s10672-007-9030-0.

34 Sofia Rebrey, 2023, "Gender inequality in Russia: Axial institutions and agency," *Russian Journal of Economics*, vol. 9, no. 1, https://doi.org/10.32609/j.ruje.9.94459.

35 Vladislav Krivoshchekov, Olga Gulevich, and Ilia Blagov, 2021, "Traditional masculinity and male violence against women: A meta-analytic examination," *Psychology of men & masculinities*, vol. 24, no. 4, p. 346, https://psycnet.apa.org/doi/10.1037/men0000426.

36 Mark James, Xue Yang Colemean, and Jessica Li, 2021, https://psycnet.apa.org/doi/10.1037/men0000426Comparison of cross-generational work values of the millennial generation and their parents in the People's Republic of China," *International Journal of Sociology and Social Policy*, vol. 41, no. 5/6, https://doi.org/10.1108/IJSSP-04-2020-0134.

James, Colemean, and Li in their own survey with a sample of Chinese millennials and older Chinese participants found that family environments including generational family members still appeared to mediate some of this difference in approach to employment and whatever might be considered most important. Those findings are still important when considering what kind of motivations might influence a Chinese cybercriminal involved in cyber espionage who has discovered wrongdoing, because they may be responsive to their generational motivations as much as they might be responsive to the kind of motivations that their parents still consider most important.

But whistleblowing is a complex phenomenon. Keenan's findings were significantly different in the early 1990s, which reflected those generational differences in Chinese communities then. Zhang, Chiu, and Wei continued an empirical examination of the decision-making process of internal whistleblowing behavior in some of these Chinese business communities, suggesting that aligning public anti-corruption campaigns could be influential in motivating reporting intention and reporting.[37] Their study like Keenan's results found that younger employees in Chinese banking sectors who had lower positions and less time with a company were more likely to report wrongdoing or fraud. Older employees were less likely to report. Zhang, Chiu, and Wei, however, cautioned highlighting these results as suggestions of distinct generational differences in Chinese communities and culture, as the study found that generally the mean number of respondents scored on the lower end of reporting wrongdoing. Zhang, Chiu, and Wei also found that someone's perception of the ethical culture of their organization in China was a significant factor in their decision to report or not report fraud.

This practitioner's paper suggests that cybercriminals originating from China or similar cultural contexts may also weigh the ethical nature of government agencies they are conducting cyberespionage on behalf of, even if those cybercriminals are also engaged in criminal activity. Someone's whistleblowing intention is largely dependent on their attitude toward reporting fraud and if they believe they have an opportunity to report fraud safely. Batishcheva and Vorontsov characterized a spectrum of concerns related to someone deciding to "blow the whistle",[38] including expression of perceptions of wrongdoing and fear of retaliation for whistleblowing. Their paper included a whistleblowing gradient for Europe based on a 2012 study among non-governmental organizations that detailed whistleblowing protections and laws in European countries. Norway and Switzerland had a high level of protections for public and private sectors, while countries like Ireland and Sweden had a level characterized as low. There were no laws or protections of whistleblowers at the time in countries like Finland and Spain, as examples. Spain included a modification in 2010 to the Penal Code that introduced protection for people reporting acts of bribery, but that modification had limited scope and no procedures in place.

Batishcheva and Vorontsov highlighted that the same list included Russia, which had no single, comprehensive legal framework for whistleblower protection. Because of the

37 Zhang, Chiu, and Wei, 2009

38 Maria Batishcheva and Viacheslav Vorontsov, 2013, https://psycnet.apa.org/doi/10.1037/men0000426Whistleblowing across Europe: it seems a gradient from West to East, from North to South. What lessons to be learned," *Summer*, vol. 33, no. 2, p. 9.

reported high level of corruption in Russia, Batishcheva and Vorontsov encouraged the introduction of whistleblower protections that aligned whistleblowing legislation and cultural practices. This paper suggests modeling or demonstrating peer behaviors could encourage those practices, even if the modeling is by cybercriminals.

People tend to seek more trusted external options for whistleblowing when they fear retaliation. Many of the whistleblowers in the Russian Olympic doping scandal were Russian athletes and Russian coaches. Barkoukis found that Russian athletes seemed to generally be more aware or informed of where and how to report misconduct, which can make a difference in terms of reporting intention and wrongdoing.[39] Russian athletes in this example arguably faced greater relational and cultural pressures and consequences from whistleblowing, but many of them did report wrongdoing. British and Greek athletes in contrast appeared to be less informed about methods and procedures for whistleblowing on misconduct.

Oelrich and Erlebach[40] agreed with Rehg et al.[41], who found that the female participants in a study on whistleblowing expressed less trust in organizational processes and protections, fearing negative consequences for their careers in addition to the increased disadvantages female employees generally tend to face compared to their male colleagues. Female participants in the Rehg et al. study were less inclined to report wrongdoing to internal authorities and more likely to pursue an external option. Oelrich and Erlebach emphasized that in nearly every situation when there is an intention to disclose information, there must also be an option to safely and securely disclose or share that information. Oelrich and Erlebach found in their own study of Chinese and Indian employees that when there was a higher fear of retaliation, there was a correlating higher motivation to report that fraud outside an organization. About half of the study participants said if they came across severe examples of fraud and corruption, they would report it.

What influence do models of shame and guilt have in different cultures?

There is a range of negative affect or "mechanisms of persuasion" that can motivate behaviors, although people do not generally explore the influence of negative emotions like guilt and shame, for example. This paper considers these emotions because of their contextual influence in cultures originating in Russia and China, where arguably in the United States

39 Vassilis Barkoukis, Dmitry Bondarev, Lambros Lazuras, SSabina Shakverdieva, Despoina Ourda, Konstantin Bochaver, and Anna Robson, 2022, "Whistleblowing against doping in sport: a cross-national study on the effects of motivation and sportspersonship orientations on whistleblowing intentions," *Journal of Sports Sciences*, vol. 39, no. 10, https://doi.org/10.1080/02640414.2020.1861740.

40 Sebastian Oelrich and Kimberly Erlebach, 2021, "Taking it outside: A study of legal contexts and external whistleblowing in China and India," *Asian Journal of Business Ethics*, vol. 10, no. 1, https://doi.org/10.1007/s13520-021-00125-y.

41 Michael Rehg, Maria Miceli, Janet Near, and James Van Scotter, 2004, "PREDICTING RETALIATION AGAINST WHISTLE-BLOWERS: OUTCOMES OF POWER RELATIONSHIPS WITHIN ORGANIZATIONS," in *Academy of Management Proceedings*, vol. 2004, no. 1, pp. E1-E6, Briarcliff Manor, NY 10510: Academy of Management.

there appears to be a highly reported frequency of cybercrime or cyberespionage. The research included below derived from Russian and Chinese communities is both qualitative and quantitative, although the empirical findings are largely based on questionnaires or surveys online. We recognize there are limitations to each of these studies. The sampling is limited in some examples and perhaps limited further by the communities sampled for those studies. As such, we generally consider these findings to be theoretical extrapolations of the frameworks or concepts that we refer to in this research. Guilt is an example of a motivating emotion that someone can use to influence behavior. O'Keefe found that there is an interpersonal character to guilt because the feeling of guilt is generally associated with hurting or anticipating hurting someone we are in a relationship with.[42] O'Keefe referred to Baumeister et al. (1994) who emphasized that guilt is strongest as a mechanism of persuasion in the context of committed relationships or interaction with people.[43]

O'Keefe included in his review and characterization of guilt as a mechanism of persuasion the influence of anticipated guilt in shaping behavioral intentions and decisions.[44] While O'Keefe noted that there are limitations to anticipating what kind of framing of anticipated guilt will influence someone's behavioral intentions or decisions, he suggested that anticipated guilt could still have the same kind of influence on someone as actual guilt feelings. O'Keefe did emphasize that anticipated guilt and actual guilt are also distinguishable, considering that someone can anticipate feelings of guilt but still not yet experience guilt. O'Keefe raised the conceptual similarities between feelings of dissonance and feelings of guilt, but he suggested that dissonance is a motivating psychological state, whereas guilt could be thought of as a "folk-psychological" term applied to contexts of feelings of dissonance.

Grigoryan et al. asked a sample population of Russians in Russia about their experiences of group-based guilt and shame regarding Russia's invasion of Ukraine, finding that only moral shame appeared to have any influence on their attitudes against war.[45] In the context of this study, moral shame meant that from the perspective of an outgroup, an attitude toward trying to prevent war because of the personal loss experienced during war was a positive attitude. The contrasting perspective in this study was image shame, which was defined as outgroup attitudes towards Russians generally when characterizing Russia as the aggressor in the conflict with Ukraine. The study found imagining shame had little influence. He explored whether there was a difference between individual ingroup attitudes toward the war and ingroup group attitudes toward the war. While most participants reported no past anti-war demonstrations such as protesting publicly against a war, he found that participants who claimed they did believe that groups can be influenced appeared more likely to change their attitude toward the war.

42 Daniel O'Keefe, 2000, "Guilt and social influence," *Annals of the International Communication Association*, vol. 23, no. 1.

43 O'Keefe, 2000, p. 99

44 Daniel O'Keefe, 2002, "Guilt as a mechanism of persuasion," *The persuasion handbook: Developments in theory and practice*, vol. 329, p. 344.

45 Lusine Grigoryan, Vladimir Ponizovskiy, Marie Weißflog, Evgeny Osin and Brian Lickel, 2023, "Guilt, shame, and antiwar action in an authoritarian country at war," *Political Psychology*, vol. 46, no. 1, https://doi.org/10.1111/pops.12969.

The beliefs about whether groups can change or that groups are responsive to guilt and shame is somewhat related to conditioning, regarding whether people believe they have control or responsibility over their governments' decisions, Grigoryan et al. wrote. This nuance was notable because, observationally, most prominent Russian personalities and other Russian influencers appeared to claim they did not feel guilt or shame from the invasion. But when a broader public narrative appeared to emerge suggesting that at some point all Russian citizens bear some responsibility for the continued decisions of the Russian government, some of those sampled attitudes appeared to soften.

Rabogoshvili et al. framed some of the similarities they believe that Russian and Chinese Generation Z share, such as their parents struggling with financial challenges but then experiencing a boost in digital technology availability and use and financial development.[46] Generation Z has grown up in environments where online social media and accessibility is the norm. Rabogoshvili et al. suggested based on their interviews and surveys with Generation Z in both countries that Chinese and Russian youth have different "models of consumption" than other generations, such as material wants and fashion on social media and money spent on them. These researchers asked Chinese and Russian Generation Z what values are most important in life – some of the top responses were justice, family wellbeing, health, and personal freedom. We suggest these values are foundational to influencing cybercriminals involved in cyber espionage to disclose wrongdoing or fraud they come across if people are being mistreated. Chimenson et al. revisited Hofstede's earlier work on general cultural characteristics, arguing that Russian and Chinese cultures are better understood through a "Yin–Yang" framework, wherein paradox and change in Russian cultural values coexist.[47] Chimenson et al. referred to traditional Russian and Chinese sayings that suggested standing out in these collectivistic cultures was not positive, however despite these social roots there is still a growing desire for individualistic pursuits among young generational Russians and Chinese. Chimenson et al. wrote that there is a "need to supplement the either/or dimensional approach to cultural understanding with a dynamic Yin Yang perspective that can capture the profound complexities of Russian culture."[48] This so-called paradox may be more of an interdependent frame for understanding similar perspectives on shame and guilt in both Russian and Chinese families and cultures.

Wong and Tsai differentiated some assumptions of established models of shame and guilt, especially in mostly western cultures.[49] Wong and Tsai noted the reported high levels of shame in some American samples that have been linked to mental illness and physiological stress and other avoidance and withdrawal behaviors. Guilt in western cultures also

46 Artem Rabogoshvili, Mikhail Bresler, Svetlana Galiullina, Daria Gerasimova, and Elena Safina, 2022, "Global similarities and glocal differences of generation Z in China, the US, and Russia: comparative analysis," *Bulletin of Ufa State Petroleum Technological University: Science, Education, Economics; Series: Economics*, vol. 3, no. 41.

47 Dina Chimenson, Rosalie Tung, Andrei Panibratov, and Tony Fang, 2015, "The paradox and change of Russian cultural values," *International Business Review*, vol. 31, no. 3, 101944, https://doi.org/10.1016/j.ibusrev.2021.101944.

48 Chimenson, et al., 2015.

49 Ying Wong and Jeanne Tsai, 2007, "Cultural models of shame and guilt," *The self-conscious emotions: Theory and research*, vol. 209, p. 223.

typically leads to some kind of response. Shame is not only viewed as an appropriate emotional response to failure within generally collectivistic models of shame and guilt, but the feeling is also valued. Wong and Tsai found in cross-cultural studies that shame may influence more response from people in collectivistic contexts, than guilt. Whereas generally Americans often view shame as negative, Chinese populations, for example, are more likely to consider shame as positive because it is socially constructive and culturally consistent. Chinese parents, for example, are generally more likely to shame their children in front of strangers discussing their children's failure than American parents, because shaming their children will likely socialize them to behavior properly.

Bedford and Hwang referred to earlier conceptualizations of guilt and shame, which suggested that shame developmentally preceded guilt, or that shame was considered more of a childish regression while guilt was thought of as a more controlled adult emotion.[50] Recent studies suggested similar outlooks that associate shame more often with something negative and maladaptive and that associate guilt with something positive.

Bedford described some of the different meanings in Mandarin for shame and guilt.[51] Bedford referred to Creighton[52] who claimed that the emotions of guilt and shame are so important for social control that it is unlikely that any society could be maintained without them. Bedford had Taiwanese female interviewers ask Taiwanese female participants what they thought of when the interviewer said the word shame or said the word guilt. The interviews revealed several forms of guilt described with different Mandarin words, such as failure to uphold an obligation to someone as well as moral and legal transgressions. Additionally, the interviews revealed several forms of shame. These forms included loss of personal reputation and failure to obtain an ideal version of self, and personal and social failure. The loss of reputation or *diu lian* was especially feared because in this context it often involves some withdrawal of community acceptance and support, Bedford wrote. As an example, a wronged customer threatening to expose an unfair shopkeeper to his or her community could induce *anticipated* loss of reputation in this context, Bedford wrote.

A form of shame defined as personal failure referred to as *xiu chi* was considered one of the strongest forms of shame in this culture. Bedford wrote that this could be called "deep shame."[53] This could include making someone else feel "deep shame" because of something you did. Bedford used an example of the parents of a girl and her community finding out she had a sexual relationship before she got married or that she got a divorce, meaning her parents will feel shame because of her behavior or circumstance and because people will believe the parents are responsible, too, because they should have raised her differently.

Bedford wrote that exposure is common to all forms of shame revealed in the interviews, whether people have found out or they might find out. Bedford referred to several

50 Olwen Bedford and K.K. Hwang, 2003, "Guilt and shame in Chinese culture: A cross-cultural framework from the perspective of morality and identity," *Journal for the Theory of Social Behaviour*, vol. 33, no. 2, https://doi.org/10.1111/1468-5914.00210.

51 Olwen Bedford, 2004, "The individual experience of guilt and shame in Chinese culture," *Culture & Psychology*, vol. 10, no. 1, pp. 31-35, https://doi.org/10.1177/1354067X04040929.

52 M.R. Creighton, 1990, "Revisiting shame and guilt cultures: A forty-year pilgrimage," *Ethos*, vol. 18, no. 3.

53 Creighton, 1990, p. 7.

researchers who have explored how social hierarchy in Chinese culture is generally connected to moral belief as that hierarchy is part of the natural cosmic order. There does not appear to be the same kind of connection to moral belief for many Westerners, but arguably there are other frameworks to consider in the military.

Proposing an integrated conceptual model of narrative persuasion and anticipated shame and guilt

In this practitioner's position paper, we are proposing an integrated conceptual model that could be applied to how persuasive communications are crafted to influence cybercriminals decision-making, when weighing whether to disclose information or not to expose wrongdoing. We are suggesting that modeling and storytelling real and imagined whistleblowing or disclosure choices by cybercriminal peers when confronted with anticipated shame or guilt could effectively encourage whistleblowing behaviors among cybercriminals.

Anticipated regret reflects what someone believes they may experience after making a choice, when they know they will find out the result of what the other choice may have been.[54]As the difficulty of a decision increases, individuals become more likely to factor anticipated regret into their choice. That decision must be individualized to be persuasive.[55] Someone's behavioral intention may be one of the most immediate and demonstrated suggestions of anticipated behavior but introducing the anticipated regret someone may experience can significantly influence that intention.[56] Anticipated guilt and shame could still have the same kind of influence on someone as actual guilt or shame feelings.[57] There are a range of broad taxonomies of "mechanisms of persuasion" that explain how affect and information processing shape decision making, but generally there must be a belief in the capability to do something in response to those "mechanisms" for that appeal to be effective. That affect and information processing could be amplified by situational contexts and the life experiences of that cybercriminal.[58]

Narrative persuasion is a form of persuasive communications, where a coherent story with characters people may identify with share an experience that may be fictional or not about something that happened, and what they did or did not do and what happened as a result. Narrative persuasion is often more influential than informational logical appeals.[59]

54 Grant Gelberg, 2002, "Regret theory-explanation, evaluation and implications for the law," . *Mich. JL Reform*, vol. 36, p. 183, https://repository.law.umich.edu/mjlr/vol36/iss1/5/.

55 Marcel Zeelenberg, Kees van den Bos, Eric van Dijk, and Rik Pieters, 1999, "The inaction effect in the psychology of regret," *Journal of personality and social psychology*, vol. 82, no. 3, p. 314, https://doi.org/10.1037/0022-3514.82.3.314.

56 Icek Ajzen, Martin Fishbein, Sophie Lohmann, and Dolores Albarracín, 2018, "The influence of attitudes on behavior," *The handbook of attitudes, volume 1: Basic principles*, pp.197-255.

57 Barbara Mellers, Alan Schwartz, and Llana Ritov, 1999, "Emotion-based choice," *Journal of experimental psychology: General*, vol. 128, no. 3, p. 332, https://doi.org/10.1037/0096-3445.128.3.332.

58 John Wilson, Boris Droždek, and Silvana Turkovic, 2006, "Posttraumatic shame and guilt," *Trauma, Violence, & Abuse*, vol. 72, no. 2, https://doi.org/10.1177/1524838005285914.

59 Anne Hamby, David Brinberg, and Kim Daniloski, 2017, "Reflecting on the journey: Mechanisms in narrative persuasion," *Journal of Consumer Psychology*, vol. 27, no. 1, https://doi.org/10.1016/j.jcps.2016.06.005.

Even fictional stories can "transport" people and influence their worldview, if those characters are like them in some way or have experienced similar contexts.[60] Transportation in this framework generally means how someone imagines or thinks about a character in a real or fictional story and how that character may reflect some part of their life or may resonate with an experience they have also had. Identification with the character in a story is complex – "processing fluency" may explain better how and why narratives and non-narratives are persuasive, meaning when a character's story is told simply and clearly people may understand that story better and may be more influenced by that story as a result.[61]

Transportation is better characterized as something experiential and based on that person's responsiveness or need for affect, rather than the kind of analytical or critical thinking processes of those elaboration or heuristic models. Some transportation scales have suggested that stories or narratives during an experience of transportation can singularly influence how someone reconsiders facts and how someone behaves.[62] Scaglioni et al. almost a decade later studied how a video made to inform people who might be eligible for colorectal cancer screening influenced their thinking and feeling about getting screened and their attitude toward getting screened.[63] This study found that the video was effective because it included an "experience" component such as what the screening was like, a "process" component such as how the character in the narrative decided to get screened, and an "outcome" component such as the expression of feelings of relief by the character in the video after getting screened for cancer.[64] Scaglioni et al. suggested that a more limited form of narrative persuasion may not have been as effective for transportation or a subsequent change in attitude or behavior. Appel and Richter added that transportation should not be confused with elaboration or heuristic models.

Positive story endings can enhance reflection, but cautionary tales can make people respond more than a positive ending.[65] The influence here is how people create meaning from narratives because of a story. Some people may reflect longer on a positive narrative because they want to "maintain the positive emotional state" from that narrative. Appel and Richter also found that someone's "need for affect" and transportation during a narrative seemed to determine how they transported or responded to a real or fictional

60 Anne Hamby and David Brinberg, 2018, "Alternative 'Facts': The Effects of Narrative Processing on the Acceptance of Factual Information," *Advances in Consumer Research*, vol. 46, pp. 498-9.

61 Olivia Bullock, Hillary Shulman, and Richard Huskey, 2021, "Narratives are persuasive because they are easier to understand: examining processing fluency as a mechanism of narrative persuasion," *Frontiers in Communication*, vol. 6, p. 719615, https://doi.org/10.3389/fcomm.2021.719615.

62 Markus Appel, Timo Gnambs, Tobias Richter, and Melanie Green, 2015, "The transportation scale–short form (TS–SF)," *Media psychology*, vol. 18, no. 2, https://doi.org/10.1080/15213269.2014.987400.

63 Giulia Scaglioni, Angela Chiereghin, Lorena Squillace, Francesca De Frenza, John Kregel, Carmen Bazzani, Francesca Mezzetti, and Nicoletta Cavazza, 2023, "Didactic and narrative persuasion: An experiment to promote colorectal cancer screening," *Applied Psychology: Health and Well-Being*, vol. 16, no. 2, https://doi.org/10.1111/aphw.12501.

64 Appel, et al., 2015, p. 511.

65 Anne Hamby and David Brinberg, 2016, "Happily ever after: How ending valence influences narrative persuasion in cautionary stories," *Journal of Advertising*, vol. 45, no. 4, https://doi.org/10.1080/00913367.2016.1237420.

narrative.[66] Highlighting controllable behaviors can influence people even more.[67]

This proposed integrated concept model of narrative persuasion and anticipated shame or guilt could be applied in any individual example, where there are cybercriminals facilitating governmental cyberespionage that could be willing to disclose or become whistleblowers related to what they interpret to be immoral acts or misconduct by the government they are supporting. Sharing these real or fictional stories of what other people like them in similar situations have done is an application of social proofing or social consensus.[68] This kind of social proof already influences cybercriminal norms, such as how someone rationalizes their own behaviors or choices in comparison or contrast to other peers in their group.

We recommend that intelligence and law enforcement agencies try to lead or manage these efforts to communicate with cybercriminals using this integrated model. While we recognize the same intelligence and law enforcement agencies historically and even recently generally underperform when attempting to communicate with or influence cybercriminals, these organizations arguably have the most resources and techniques and information to appropriately and powerfully share these narratives to motivate a response. There will always be a need to safely and securely establish communications with someone who is willing to risk so much to share information including information on wrongdoing or fraudulent activity by foreign governments. Intelligence and law enforcement agencies are positioned to do this. However, we want to emphasize that many of the possible narratives that might appeal to a broad audience of cybercriminals from different backgrounds should be openly shared in many cases, to encourage sharing and commentary from others who may also influence their response. Ultimately, if someone is willing to become a whistleblower, that contact should be confidential. There are norms for confidential or covert communications that intelligence and law enforcement agencies can support or facilitate. But many of these narratives need to be shared publicly first.

Visualizing application of this proposed integrated conceptual model

The following theoretical scenarios represent examples where this conceptual narrative model could be applied to develop behavior-based strategic messaging.

Scenario 1: Corrupt Anti-Corruption East Asian Officials

Scenario: A cybercriminal discovers or is informed that East Asian government officials who are responsible for anti-corruption measures are themselves engaged in corruption. This corruption has been impacting the lives of this cybercriminal's family members.

66 Markus Appel and Tobias Richter, 2010, "Transportation and need for affect in narrative persuasion: A mediated moderation model," *Media psychology*, vol. 13, no. 2, p. 2, http://dx.doi.org/10.1080/15213261003799847.

67 Nurit Tal-Or, David Boninger, Amir Poran, and Faith Gleicher; 2004, "Counterfactual thinking as a mechanism in narrative persuasion," *Human communication research*, vol. 30, no. 3, https://doi.org/10.1080/13576500342000013.

68 Robert Cialdini, 2009, *Influence: Science and practice*, vol. 4, Boston: Pearson education.

Anticipated shame or guilt: This cybercriminal has an opportunity to reveal and disrupt this corruption, or this corruption could continue to negatively impact the cybercriminal's family. The cybercriminal's family could eventually find out that the cybercriminal was aware of this corruption and he or she had the opportunity to reveal it.

Narrative persuasion: This modeling could include the cybercriminal's childhood and his or her love for their family, which would "transport" many of their peers in similar situations. A cybercriminal who does not try to protect his or her family even if that disclosure could result in punishment or consequence for the cybercriminal might suggest that cybercriminal is greedy. That kind of behavior can be shamed. The cybercriminal's motivation to protect his or her family and prevent further corruption from impacting his or her family could appear to be more important than whether that disclosure damages the reputation of the government or benefits a foreign government. This narrative could also be rationalized as an opportunity to protect the government from further corruption and reputational damage by exposing these corrupt officials.

Possible impact: A cybercriminal who previously or currently was facilitating cyberespionage on behalf of that East Asian government would likely have access or could gain access to verifiable data or other sensitive information that materially demonstrates corruption by these so-called anti-corruption officials. Disclosing this kind of information could not only lead to the dismissal or removal of those officials but could influence other measures by that government in efforts to manage impressions among East Asians and reputational concerns outside of this East Asian country. A cybercriminal could potentially remain anonymous in this kind of disclosure.

Scenario 2: Eastern European Officials Excluding Sons From Conscription

Scenario: Eastern European officials with power and influence have removed their own sons from military conscription, as the cybercriminal loses family members and friends to conscription in a regional conflict. There is growing public outrage because of some limited news reports from restricted Western news media and rumors that various government officials have been excluding their sons from military conscription.

Anticipated shame or guilt: Some in the public have started vocalizing the loss of their sons in this regional military conflict. Some family members and friends of this cybercriminal have started joining those protests. There are opponents of some of these officials who have threatened to pursue proof of how these corrupt officials excluded their sons from conscription. This cybercriminal worries that there could be records found that suggest this cybercriminal is associated with these corrupt officials, because of cyberespionage this cybercriminal has facilitated for them. This cybercriminal has knowledge of the location and access methods to restricted databases that would hold the kind of 'proof' the public and political opponents have been looking for.

Narrative persuasion: This modeling could include cautionary tales featuring real or fictional cybercriminals who have been in similar situations in the past where they had an opportunity to reveal information that might have disrupted any further wrongdoing or harm to the public or their own friends and family, but they did not reveal that information and their loved ones were hurt. This narrative could also be rationalized as an opportunity for a growing collective of Eastern European cybercriminals and gangs who have likewise lost family members and friends to this military conflict because of conscription to challenge the government's power and corruption, even if that interdependent relationship between the government and cybercriminals is tenuous.

Possible impact: A cybercriminal with knowledge of the location and access methods to the kind of material that could confirm these government officials were using their power and influence to exclude their sons from conscription could carefully extract this content, including masquerading as anticipated political opponents or foreign governments who would also be interested in this information. Disclosing this kind of information could enable global news media and other organizations to project these material claims of corruption and force this Eastern European government leadership to mitigate that corrupt practice and perhaps reduce conscription. Reduced conscription could ultimately impact the nature of the regional military conflict as well.

Discussion

There is still a considerable and understandable stigma toward cybercriminals, but perhaps some of that fear borders on folklore of the threat of any Russian- or Chinese-speaking cybercriminal. There are some parallels to how Japanese communities and Japanese-Americans were characterized in terms of threat throughout the world when there were limited and biased collection and analysis of observed Japanese communities, even when there were understandably preparations by the Japanese government to eventually start conflict in Southeast Asia. This example is not intended to diminish the contemporary threat assessments of nation state attackers and governmental efforts engaged in cyber espionage, but it may be helpful providing some alternative framing on how the communication of folklore and our myth making can influence how we characterize or mischaracterize threats and then act on those characterizations.

Everest-Phillips reexamined the pre-World War II fear of Japanese espionage around the world and how that fear and resulting characterizations of Japanese activity in many cases embellished the threat of Japanese presence.[69] This examination is a useful model for reconsidering some of the characterizations of not only whistleblowers but also cybercriminals engaged in cyberespionage for criminal profit or for foreign governments. Everest-Phillips found that the exaggerated 'threat perception' of Japanese activity especially throughout Southeast Asia had some basis in prejudicial views communicated by European and American interests in that region and the surrounding region given Japan's sudden rise as a

69 Max Everest-Phillips, 2007, "The pre-war fear of Japanese espionage: Its impact and legacy," *Journal of Contemporary History*, vol. 42, no. 2, https://doi.org/10.1177/0022009407075546.

major regional power in the years before World War II. The reports and characterizations of Japanese activity in the form of Japanese businesses and tourists came to represent "part of the vast web of commercial espionage which Japan had spread over the areas she planned to dominate", Everest-Phillips wrote, quoting an Australian intelligence report of Japanese intelligence activity published in the late 1940s. These observations and analysis seemed to suggest there was systematic espionage across the region, which Everest-Phillips wrote "acted as both a symptom and a cause of international hostility".[70]

Everest-Phillips wrote that because of the worsening relations between the western powers and Japan between the world wars, "the myth of Japanese espionage was a powerful force".[71] Exaggerations increasingly distorted impressions and threat characterizations of Japanese capabilities and dormant or non-threatening Japanese activity and later seemed to affirm those suspicions when the Japanese did eventually launch attacks in that region. This distorted "conspiracy of armed aggression" and suspected Japanese espionage over influenced the American and allied response to Japanese communities before and during war.[72] We suggest in this paper that the struggle among many organizations and governments to respond to or manage cybercriminal threats and activity originating from Russian- and Chinese-speaking hacking collectives and nation states, may be influencing attitudes toward engaging some of these same cybercriminal personalities to encourage whistleblowing and cooperation.

Several of the whistleblowers in the Russian Olympic doping scandal were Russian athletes and Russian coaches. Barkoukis et al. found that Russian athletes seemed to generally be more aware or informed of where and how to report misconduct, which can make a difference in terms of reporting intention and reporting that wrongdoing.[73] Russian athletes in this example arguably faced greater relational and cultural pressures and consequences from whistleblowing, but many of them did report wrongdoing. Some of that influence may have been a result of their own anticipated guilt or shame if they did not report that wrongdoing. British and Greek athletes in contrast appeared to be less informed about methods and procedures for whistleblowing on misconduct, based on Bondarev et al.'s study. Lacking information on how to safely disclose this kind of information could be a considerable challenge to someone deciding whether they will become a whistleblower or not.

We argue in this practitioner's position paper that while these examples of disclosing wrongdoing have grown considerably in the past decade and there is a growing awareness of options for safely and securely disclosing information revealing misconduct, there are still limited examples highlighting the decision making of these whistleblowers among cybercriminals. We recognize there also may not be many examples of whistleblowing among cybercriminals facilitating cyberespionage for governments, for many understandable reasons. These could include the secrecy of their role and the consequences of revealing misconduct by the government they are supporting. In some cases, those consequences may

70 Everest-Phillips, 2007, p. 245.
71 Everest-Phillips, 2007, p. 264.
72 Everest-Phillips, 2007, p. 264.
73 Barkoukis, et al., 2022.

involve death. This proposed integrated conceptual model for encouraging cybercriminals in these situations to become whistleblowers or disclose information of fraud and corruption or worse to the public for the benefit of the public could result in more of this behavior.

We argue that the influence of social proofing or social consensus has been underestimated in these contexts and perhaps the influence of social norms among cybercriminals has been unchallenged. This paper has suggested that a root explanation for why there has been a lack of messaging to cybercriminals to encourage them to use their extraordinary access and skills for the benefit of the public when faced with wrongdoing and misconduct by governments is because cybercriminals are generally characterized as linear in motivation to only profit. We argue from experience that cybercriminals are no different than most, struggling with similar motivations and choices related to their relationships and themselves to help and protect others.

Authors

Tim Pappa is an Incident Response Engineer - Cyber Deception Strategy, Content Development, and Marketing, Cyber Deception Operations, Walmart Global Tech. Before Walmart Global Tech, Tim was a Supervisory Special Agent and profiler with the Federal Bureau of Investigation's (FBI) Behavioral Analysis Unit (BAU), where he specialized in cyber deception and online influence. Tim has presented and published at various academic and industry conferences, including Black Hat Asia, NDSS, IEEE SP, CYBERWARCON, and the Honeynet Project. Tim has also held various strategy and policy Fellow roles at the Center for Strategic and International Studies (CSIS) and the Aspen Institute. Singapore-based publisher, World Scientific, published his first book, "Influencing the Influencers: Applying Whaley's Communication and Deception Frameworks to Terrorism and Insurgent Narratives" in summer 2025. He is currently writing No Starch Press's first book on cyber deception.

Olga Kuprina is a researcher in web/system/networks attacks on various platforms, with strong focus on penetration testing, social engineering, and human intelligence (HUMINT). Her twenty-two years of experience in hacking, insider trading, carding, corporate espionage, fraud, and related cybercrime activities include having been the leader of an elite international Ukraine-based hacking organization. Undetected for years, silent network intrusions earned her the nickname "Ghost in the Shell." Her criminal resume includes hacking into SEC.gov, Pentagon and NASA, and her social engineering skills include five years of successful undercover work, distruption of several of the most notorious ransomware gangs, creation of underground community, and managing social media disinformation campaigns. Olga has a well-known in criminal history as "The Number One Hacker in the World."