Position Paper: The amplification of online deviancy through the language of violent crime, war, and aggression

Alice Hutchings
Director, Cambridge Cybercrime Centre
Department of Computer Science & Technology
University of Cambridge
Cambridge, UK
alice.hutchings@cl.cam.ac.uk

***Abstract*—Cybercrime has long been romanticised, by the media, academics, politicians, and the computer security industry. Depictions of cybercrime use evocative language, often deeply related to violence and war. The lived reality, for victims, offenders, and defenders, is often vastly different. I argue that we should not be using terms of violence to describe cybercrimes, the vast majority of which are low level, automated, and financially driven. While the violent rhetoric may capture our imaginations, it undermines the lived realities of the victims of atrocities and provides a warped view into the world of cybercrime.**

***Index Terms*—Cybercrime, language, war, violence, aggression**

Content warning: Contains graphic references to sexual assault and violence.

When we think of cybercrime, we often imagine the most catastrophic outcomes. When Russia invaded Ukraine in February 2022, there was speculation civilian-led online attacks would escalate into a full-blown cyberwar. An eminent criminologist went as far as to conjecture that a bumbling hacker mistakenly making their way into the controls for nuclear weapons would lead to nuclear war [1]. At the Cambridge Cybercrime Centre, we have been collecting data relating to online attacks for many years, so we turned our attention to measuring this anticipated increase and change in the nature of online attacks.

What we found challenges this popular narrative. While there had been a slight increase in website defacement and denial of service attacks targeting Russian and Ukrainian infrastructure, beginning just hours after the invasion began, this only lasted several weeks. Compared to the global scale, the level was minuscule. We interviewed some of those responsible for the website defacements and learnt that the majority of their activities are not targeted. Indiscriminately, using automated approaches, they identify websites with well known vulnerabilities. They are motivated by fame (hence their willingness to talk to us), but also financially, advertising cybercrime tools and services on the defaced pages [2]. Overall, this pattern fits with other research that finds much cybercrime consists of low-level offending, using well-known exploits and automated tools, rather than sophisticated attacks [3].

Overall, crime is changing, in multiple ways. Cybercrime now accounts for about half of all property crime [4]. This is particularly astounding given the limited police budgets to address the problem. The violent crime landscape is also changing, although on a longer timescale. Pinker [5] documents how we are now living in some of the most peaceful times in human history. While atrocities such as the invasion of Ukraine dominate our headlines, if we look at the bigger picture, humankind has evolved. The vast majority of people now live in relatively peaceful societies governed by rights and ethics, not experiencing wide-scale acts of aggression and war.

The language used to describe cybercrime and computer security is not borrowed from the offline phenomena (property crime) it replicates. Instead, it reflects violent crime, war, and aggression. In doing so, it demeans the lived experiences of those that do suffer horribly at the hands of aggressors. For example, *'fraping'* [6], or altering a Facebook page, is not the same as being brutally raped. I concede there are some similarities. Both are most likely to perpetuated by someone known to the victim. Both cause harm. Both are under-reported. However, momentarily changing someone's social media page, sometimes just as a prank, is not the same as being physically assaulted. A violent sexual assault causes immediate physical harm, is associated with ongoing PTSD and other mental health concerns, and can be life changing to the victim. Online harassment can still cause a range of harms, some serious, yet is a fundamentally different crime with different reactions. Equating the two is a disservice to both crimes.

Language is evocative and powerful. The words we choose activate our imaginations. The language we use affects our psychology, our society, and our culture. It sways how we feel and how we respond. The words we use are important. Words can perpetuate harms. The shift away from using terms like 'master' and 'slave', 'blacklist' and 'whitelist' is an example of a realised harm that is now being addressed by the computer security community [7]. Similarly, it is now readily accepted that referring to child sexual abuse material as ‘child pornography’ is an inaccurate and harmful term that normalises the sexual exploitation of children.

The private sector security industry does not choose its words lightly, deliberately creating a militaristic mystique around themselves. War and violence are used to wield power over others. Perhaps this is the idea behind using words associated with violence; to be evocative and to assert control. Indeed, the idea of war is the populist politician’s exploitative fantasy. Dressed in army fatigues, delivering rousing addresses to the nation. Being remembered in history, having ice cream (Napoleon)[1] and Cambridge Colleges (Churchill) named after them. Their likeness replicated in bronze for generations to admire. Violence is not entertainment. Yet it is, depicted in horrors and thrillers and dramas; uncomfortably long fight scenes. In reality, violence is not glamorous. It is gritty, dirty, painful, and demeaning.

A computer intrusion is an *attack*. Targets are *hit*. Perpetrators are called *hackers*. While it is argued the term hacker comes from tinkering or playing with technology in fun and creative ways, the older meaning of the word hack is to use rough or heavy blows to cut something or somebody. I argue that the use of this terminology is harmful. Executing code is not a direct analogy to a violent or aggressive act.

Trying multiple usernames and passwords represents a *brute force attack*. But despite the connotation, there is no power element here. The term brute force has been borrowed by the information security community, but its application does not have any associated element of physical violence. Websites are *defaced*, a particularly puzzling term given websites are not commonly considered to have faces! While the term is used in the physical world to describe spoiling treasures or artefacts, this often requires physical strength, rather than technical know-how.

Nowadays, new and innovative vulnerabilities are marketed, a co-ordinated vulnerability disclosure comes with media releases, flashy logos, and impressive websites. Camp [8] explored the use of different mental models and how they may affect risk perception. She notes the warfare metaphor has been ‘internalised’ by the computer security industry. Names such as *Heartbleed*, *Rowhammer*, *BashBug* and *Shellshock* are being deliberately chosen. If we reflect on these terms, we notice they represent injury and tools of violence and war. Similarly, *bombs* cause horrendous harm, including death, serious injury, and destruction to all around. They can be dropped from the sky, hidden in landmines, or thrown as grenades. They can vary in sophistication and scale from the Molotov cocktail–accessible to all–to the atomic bomb. It is a far stretch to argue that *logic bombs, fork bombs, email bombs*, or *zip bombs* create terror and destruction to the same extent.

Computer scientists seem to enjoy Greek mythology. Consider the *Zeus* banking *trojan*. Zeus, chief of the Greek gods, was the father of Ares, the god of war. And *trojan* comes from the story of the Trojan horse, a gift used to hide soldiers to invade the city of Troy. Today’s Trojan is a malicious payload hidden in a seemingly innocent file designed to entice the user. The Zeus banking trojan, despite its name, is not a tool of war. It is a tool designed to steal from people’s bank accounts, a financial (property), not violent, crime.

Should we consider cybercrime tools in the same way we consider tools used for violence and oppression? The latter have more visual impact. Recently, the world turned in horror to the atrocities in Ukraine, to tanks rolling down streets, to the smoke of bombs. Photos of civilians, shot in the head, lying in the streets with their white armbands. Bodies of naked women, hidden by a blanket, found by a roadside. The entire family of a local politician killed and partially buried. Stories of bravery, repelling invaders, stepping before tanks, saying ‘Russian warship, go fuck yourself’.

Perhaps this lack of evocative visual imagery is precisely why violent terms are used in computer security. We cannot so easily conjure the public imagination by providing images of the harms caused by computer code. Images of hooded or masked men quickly become trite. Instead, we use ‘fear appeals’ [9], inviting such visual imagery by using terms associated with violence and aggression. Maybe we are doing so to say, this is serious, something needs to be done about it. Pay attention!

There are dangers to using evocative language to describe what are often mundane activities of cybercriminals. It often criminalises and catastrophises pretty trivial forms of teenage deviance. It repurposes cybersecurity away from what might be quite a communitarian, solidaristic thing of communities coming together to help each other out and turns it into a high security, command-and-control phenomenon. It provides an exciting view of cybercrime that belies the often rote, boring reality for those whose main job is dealing with administrative tasks [3]. By making cybercrime appear more risky and exciting, it potentially attracts new actors keen to start smashing stacks [10]. But also, it can alienate the general population to the risks they pose. Cybercrime is then seen as being the purview of national states, in response to high impact incidents. This does not reflect the reality of petty actors who do not possess impressive coding skills but use well-worn exploits and toolkits to steal credentials at scale.

Another danger is the persisting gender divide in the computer security industry, where women are under-represented. Gender roles, like language, are socially constructed. If we view security through the analogy of war, men are soldiers, standing tall. Machine guns held by muscled arms. Women are nurses, tending the wounded. Holding thermometers and bandages, caring for all. But these are just perceptions; with the contributions made by women to the war effort, such as code breaking, largely written out of history. Computing was generally seen as women’s secretarial work, but this changed once it became clear there was going to be big money in it [11]. It is rarely the case that the difference in physical strength between women and men is key to winning or losing

[1] Neapolitan icecream is probably named after the Italian city Naples, home of delicious iced treats, rather than Napoleon Bonaparte, but why let facts stand in the way of a good fictional story about Trump covfefe-flavoured Magnums.

a battle. Tactics, supply chains, coordination, correct use of equipment, etc. is all the more important. It doesn't matter whether your tank commander is a man or a woman. The same must be true for cyberspace where physical strength is an irrelevance. However, terminology that is alienating, that perpetuates the 'maleness' of force and violence, may contribute to the lack of engagement by women in the field.

In the future computer viruses and worms might in fact lead to large-scale physical damage. Perhaps 'attack' is the right word to use when terrorists use a software vulnerability in self-driving cars to send all cars of a specific make and model into out-of-control urban weapons? Perhaps, however, the point is that this is unlikely. The skill set required to do this is out of reach of most. The majority of offenders possess very little advanced technical skill. Furthermore, there is little incentive, with most offenders motivated by money rather than destruction. And while some offenders are perfectly happy to steal money from bank accounts, reasoning that it is the banks rather than individuals that bear the final cost, there is less opportunity to internally neutralise large-scale violence against citizens.

Table I lists established words commonly used in computer security that are linked to violence and proposes replacements. These will not be unfamiliar terms for many, as they are predominantly sourced from the terminology used to describe property crime. These, I believe, reflect the reality of the majority of cybercrime that compromises data and financial security.

Words of violence	Suggested replacement
Attack	Offence
Hit	Victimised
Hacker	Offender
Hack	Unauthorised access (or other descriptive term related to the activities being referred to)
Brute force attack	Systematic password checking
Defacement	Graffiti

TABLE I

Words of violence and potential replacements

I'm not arguing that changing our terminology is a magic bullet to improving the cybersecurity landscape. Inflammatory language is being used in an attempt to gain sorely needed attention. However, other approaches may be more effective. These include a mature computer security workforce that does not introduce vulnerabilities by 'moving fast and breaking things'. An ecosystem that can respond rapidly to patching existing vulnerabilities that does not rely on provocative names and catchy headlines. Police that recognise that offenders are effectively operating with impunity, that most cybercrimes are low value but high in volume, and to prioritise these. Law enforcement that can effectively collaborate across jurisdictions, something that is required for all but the most mundane cybercrimes, yet rarely needed for any but the most serious or unusual of physical crimes. We need police that are properly resourced to do this.

Like the Baader-Meinhof phenomenon [12], once you start noticing the oddity of the language we choose to use in computer security, you may start to recognise it everywhere. Of course, I should acknowledge that not all terms used in computer security suffer from these misappropriations. *Mirai* (the Internet of Things malware) was released by a forum actor using the moniker *Anna Senpai*; both names originate from Japanese Manga (with their own problems relating to the depiction of women). My overall favourite is *LoveBug*, an early computer worm that spread by pretending to be a declaration of affection. However, language is really only a symptom of a bigger problem. It reflects the status quo of our existing cybersecurity and policing communities. Change will come not only from the language we use, but how inclusive and welcoming we are.

Acknowledgment

This paper is part of a project that has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 949127).

I thank my colleagues at the Cambridge Cybercrime Centre, in particular Professor Alastair Beresford (University of Cambridge), Dr Daniel R. Thomas (University of Strathclyde), and Dr Ben Collier (University of Edinburgh), for their thoughtful insights and detailed comments.

References

[1] J. Braithwaite, "Macrocriminology and Freedom," 2022, Nigel Walker Seminar, Institute of Criminology, Cambridge.

[2] A. V. Vu, D. Thomas, B. Collier, A. Hutchings, R. Clayton, and R. Anderson, "Getting bored of cyberwar: Exploring the role of the cybercrime underground in the russia-ukraine conflict," *arXiv preprint arXiv:2208.10629*, 2022.

[3] B. Collier, R. Clayton, A. Hutchings, and D. Thomas, "Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture," *The British Journal of Criminology*, vol. 61, no. 5, pp. 1407–1423, 2021.

[4] R. Anderson, C. Barton, R. Böhme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore, and M. Vasek, "Measuring the changing cost of cybercrime," *Workshop on the Economics of Information Security (WEIS)*, 2019.

[5] S. Pinker, *The better angels of our nature: The decline of violence in history and its causes*. Penguin UK, 2011.

[6] W. Moncur, K. M. Orzech, and F. G. Neville, "Fraping, social norms and online representations of self," *Computers in Human Behavior*, vol. 63, pp. 125–131, 2016.

[7] J. E. Gilbert, S. Ludi, D. A. Patterson, and L. M. Smith, "Words matter," *Communications of the ACM*, vol. 65, no. 7, pp. 36–36, 2022.

[8] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[9] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly*, pp. 549–566, 2010.

[10] A. Goldsmith and D. S. Wall, “The seductions of cybercrime: Adolescence and the thrills of digital transgression,” *European Journal of Criminology*, vol. 19, no. 1, pp. 98–117, 2019.

[11] M. Hicks, *Programmed inequality: How Britain discarded women technologists and lost its edge in computing*. MIT Press, 2017.

[12] S. Aust, *The Baader-Meinhof Group: The Inside Story of a Phenomenon*. Bodley Head, 1987.