Defeating Digital Viruses: Lessons from the Pandemic

Dr Victoria Baines, IT Livery Company Professor of IT

21st March 2023

During the COVID-19 pandemic, public health messaging was an essential component of governments' responses.[1] Research has already been published that seeks to evaluate the effectiveness of this messaging, for example, from the perspective of Communication Science, in terms of self-reported levels of compliance, and with a particular interest in the use of social media.[2] While systematic reviews are still ongoing, as individuals we can testify that when asked to cover their faces, wash their hands, and distance themselves from each other to protect themselves, their loved ones and their communities, many people did this, and (at the time of writing in early 2023) some still do. People all over the world proved that they were capable of taking preventative measures to control the spread of infection, including getting vaccinated. In the UK, public health messaging was reinforced with memorable slogans exhorting the public to action. These included "HANDS | FACE | SPACE", "STAY HOME | PROTECT THE NHS | SAVE LIVES", and "STAY ALERT | CONTROL THE VIRUS | SAVE LIVES."

At the time, I was writing a book on security rhetoric: the techniques used by governments, the media and others to communicate safety and security issues. My research found remarkable consistency between ancient exaggerations of the dangers of living in Rome, former President Trump's hyperbolic assertions in his 2017 National Security Strategy that the world is "extraordinarily dangerous" and "filled with a wide range of threats", and the tendency of some government authorities and cybersecurity providers to catastrophise cybercrime. I was reminded of the similarity of the language and imagery of pandemics and that of cyber threats. More precisely, how the cybersecurity world routinely borrows from virology, immunology, and epidemiology to represent cyber threats as viruses and infections that spread. It set me thinking about why we had come to do that, what challenges that comparison might present, and whether there were opportunities to put it to better use.

Fear, Uncertainty, and Doubt

In my analysis of public messaging on cyber threats I compared government statements with anti-virus companies' marketing materials, and both of those to scam emails and pop-up messages written by cybercriminals. What I found really surprised me: all three used similar techniques and imagery to describe cyber threats, including darkness, anonymity, amplification of scale and impact, urgency and emergency, and mystifying technical jargon.

---

[1] With thanks to Martyn Munro for his assistance with the public health content of this lecture and transcript.

[2] Nan et al. (2021) "Public Health Messaging during the COVID-19 Pandemic and Beyond: Lessons from Communication Science". *Health Communication* 37.1: 1-19. https://doi.org/10.1080/10410236.2021.1994910. Merchant et al. (2021) "Public Health Messaging in an Era of Social Media". *JAMA* 325.3:223-224. doi:10.1001/jama.2020.24514. Basch et al. (2020) "COVID-19 on TikTok: harnessing an emerging social media platform to convey important public health messages". *International Journal of Adolescent Medicine and Health* 34.5. https://doi.org/10.1515/ijamh-2020-0111

Figure 1 Image of a cybercriminal on the FBI website (until August 2020): Shutterstock

The saying goes that a picture paints a thousand words, and this image is the epitome of public messaging on cyber threats for the last three decades. The blue light, circuitry background and cascading binary code speak of technical sophistication that is beyond the grasp of most people. The central figure appears to be a magician, conjuring up numbers from an ethereal keyboard, the like of which I've certainly never seen in real life. We're encouraged to assume that this is a man. He wears the stereotypical uniform of a hacker, the hoodie, and he is faceless. His hands are accentuated because they're the only part of his body that's visible. They are grasping, rapacious even. They encourage us to think of him as a violent criminal, a mugger or worse. But unlike the common or garden violent criminal, the map behind him suggests that he is capable of reaching right around the world.

In reality, not all cybercriminals wear hoodies, many of them don't identify as male, and all of them have faces. But somehow we've ended up in a place where this is the accepted way to represent them, and I would argue that the overwhelming impact is one of powerlessness, of helplessness, and of hopelessness. Imagery that depicts cybercrime like this does nothing to make people safer beyond pushing them to buy a product. It has more to do with fiction and fantasy than with reality. And yet, for several years, this was the 'welcome' image on the FBI's website when ordinary people searched for advice on cybercrime prevention.

Well-intentioned use of metaphors has made data, networks, and code seem more immediate and accessible. Metaphors' persuasive impact is in their ability to make people feel as they might feel about the point of comparison. For example, parts of the web are 'dark' because they are not indexed by mainstream search engines and are therefore less visible. Malicious software 'infects' a computer because it enters the machine, spreads, and impairs its functioning. It behaves *like a virus* because it self-replicates, but it does not (yet) attack human bodies.

A Brief History of Digital Virology

The viral metaphor is commonly traced back to Gregory Benford's 1970 short story "The Scarred Man", in which malicious software had the name 'VIRUS', and the program engineered to remove it 'VACCINE'.[3] Benford had worked on the precursor to the Internet, the US Department of Defense's ARPANet project in

[3] Excerpt at http://www.technovelgy.com/ct/content.asp?Bnum=2402.

the 1960s, yet another intersection between life and art, science fact and science fiction. Researcher Fred Cohen is credited with introducing 'computer viruses' to the academic world.[4] Cohen's definition was the blueprint not only for usage of the term 'virus', but of a wider transferred lexicon:

> "We define a computer 'virus' as a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows."

The hyperbolic potential is exploited from the outset. Cohen expands:

> "As an analogy to a computer virus, consider a biological disease that is 100% infectious, spreads whenever animals communicate, kills all infected animals instantly at a given moment, and has no detectable side effects until that moment. If a delay of even one week were used between the introduction of the disease and its effect, it would be very likely to leave only a few remote villages alive, and would certainly wipe out the vast majority of modern society. If a computer virus of this type could spread through the computers of the world, it would likely stop most computer use for a significant period of time, and wreak havoc on modern government, financial, business, and academic institutions."

This language taps into our deep-seated fear of death and basic physiological needs. Its transferral to cybersecurity imbues computer problems with a sense of mortal danger. In the context of a global public health emergency, such descriptions may be uncomfortable reading to a public that has endured a very real viral threat to life, and that has been instructed to be on the alert.

Alarmist public messaging at such a time is something of a gamble: target audiences may legitimately feel that they have bigger, more immediate threats to worry about; customary hyperbole may be indistinguishable from the noise of a large number of competing voices seeking to persuade citizens that they need their products "more than ever". But causing alarm is a default tactic of cybersecurity rhetoric, and old habits die hard. In late 2020, one vendor displayed the following text on their website [original emphasis] [5]:

> "*Preparing for the Next Global Crisis - A Cyber Pandemic*
>
> People and organizations have suffered greatly from the coronavirus pandemic. Many critical lessons are being learned, but none more important that [*sic*] another devastating crisis could be brewing. A catastrophic cyber event has long been envisioned, and with today's digitally connected world, a global cyber pandemic is now a reality."

A banner at the top of the company's web pages urged visitors to "Prepare for a Cyber Pandemic. Secure your everything now." There are a number of possible reactions to this content: it could indeed trigger the alarm at which it is evidently aimed; it could be rejected as a cynical attempt to exploit an already heightened state of alert; it could likewise be seen as crass and insensitive by people who have been directly affected by the real virus. We can perhaps be more definite about what this messaging is not, and that is empowering to the citizen. Governments in their communications on COVID-19 were keen to emphasise the role of ordinary people in controlling the spread of the virus, protecting themselves and others. In the text above, the only solution is to purchase the product offered by the vendor – no further protective advice is given. The final assertion of the paragraph that "a global cyber pandemic is now a reality" is intrinsically meaningless, given that we currently have no way to reliably quantify cyber-attacks worldwide, and therefore to determine whether they meet the scientific threshold for a pandemic.

On the same theme, a range of vendor solutions started to promise 'cyber-immunity'. Some providers were quick to restate their allegiance to the concept while the global community was in the throes of the first wave of coronavirus infections.[6] This period also saw the emergence of a product that claimed to be the world's first 'computer vaccine'.[7] Without the sales figures of these companies before and after this communication, it is impossible to gauge how successful these attempts to capitalise on the pandemic have been. It is clear,

---

[4] Fred Cohen (1987) "Computer Viruses: Theory and Experiments". *Computers & Security* 6: 22-35.

[5] Checkpoint (n.d.) "Protecting Against a Rapidly Spreading Cyber Pandemic". https://www.checkpoint.com/cybersecurity-protect-from-cyber-pandemic/, accessed 10/11/2020.

[6] https://www.kaspersky.com/blog/applied-cyberimmunity/28772/, accessed 10/11/2020; https://www.darktrace.com/en/press/2020/332/, accessed 10/11/2020.

[7] Atense (2020) "No More Anti-Virus Software - Atense Inc., a Cyber Defense Company Claims To Have Developed The World's First Computer Vaccine", company press release 17/06/2020. http://www.atense.com/Press_Release.html

however, that COVID-19 has been used by some in the cybersecurity industry not only as a business opportunity, but also as a device to persuade potential customers of the urgency and severity of cyber threats.

None of this critique should be taken as dismissive of the threat. Cyber-attacks can be serious and damaging, be it to reputations, finances, national security, and even personal wellbeing. Highlighting the way in which certain frames of reference are consciously chosen above others, however, and considering the potential impact of those on different audiences, especially the non-specialist public, can help us to identify alternative framings that may resonate with citizens while empowering them to protect themselves and others.

A Public Health Framework for Cybersecurity

One proposed approach seeks to harness lessons learned from public health rather than simply exploiting its language and imagery. Starting from the assertion that both public health and cybersecurity are public goods, Mulligan and Schneider (see Further Reading) have proposed a doctrine for public cybersecurity that is based on collective interest rather than individual benefit, and whose goals are to produce cybersecurity and manage the insecurity that remains. Rowe, Halpern and Lentz have elaborated an intervention model that compares communicable and non-communicable cyber threats to communicable and non-communicable diseases, cyber risk behaviours to public health risk behaviours, and environmental exposures relevant to cybersecurity and public health respectively (see Further Reading).

Category	Public Health	Cyber Security
Communicable diseases	COVID-19, hepatitis, HIV/AIDS, tuberculosis	Botnets, social media hacks, influence operations
Non-communicable diseases	Cancer, heart disease, chronic respiratory diseases, diabetes	Ransomware, denial of service (DOS), phishing
Risk behaviours	Alcohol and drug use, smoking, poor nutrition, lack of exercise	Sharing passwords, not installing anti-virus, clicking unchecked links
Environmental exposures	Hazardous chemicals, pathogens, poor sanitation, air quality	Unsecured Wi-Fi, shared devices, exposure to fake news, personal data transfer

Figure 2 Possible taxonomy for cyber public health (after Rowe, Halpern & Lentz (2012)

Following this model, communicable cyber threats such as email spoofing or unwittingly being the intermediary for an attack as part of a botnet of compromised devices are met with system-level interventions drawn from public health, including quarantine, mandatory reporting of new cases, educational information and guidelines for early detection.

Primary Prevention – avoid threat	Secondary Prevention – address threat at onset	Tertiary Prevention – prevent threat worsening

Avoid "high risk" behaviour	Scanning devices for malware	Incident reporting
Cyber hygiene measures	Removal of malware	Incident response
Software patching	Mandatory reporting	Law enforcement
Security regulations	Network/system based detection	Quarantine

Figure 3 A public health approach to cyber threat prevention (after Rowe, Halpern & Lentz (2012)

As discussed in the third lecture in this series (*How to Fight Fake News*), successful cybersecurity measures focus on people, process, and technology.[8] They are the cornerstones of how society combats cyber-attacks and cybercrimes. Cybersecurity and online safety require the active engagement of individuals, but also of the public at a societal level. In public health terms, this means public education. It also means placing importance on prevention: primary prevention seeks to minimise the threat by addressing risk behaviours and promoting generalised protections; secondary prevention seeks to reduce the impact of a disease or incident through targeted intervention; the aim of tertiary prevention, meanwhile is to manage long term effects and reduce the risk of recurrence.

A Whole Society Approach

Operating at a population rather than an individual level, public health responses are whole society responses, in which each group or population has a role. A social-ecological model recognises that an individual's history and circumstances, their relationships, their community, and society at large interact and all influence the occurrence of a problem and levels of protection from it. In my research on online child abuse a few years ago, mapping the ideal response in this way enabled me to have a holistic appreciation of the range of interventions and stakeholders required.[9] Crucially, it demands that we give equal consideration to all types of intervention, regardless of our personal preferences or aversions. For example, in order for children to be effectively protected from sexual abuse online, it isn't enough simply to make children and caregivers aware of the dangers. There also need to be services such as the StopItNow! helpline, which helps people who are concerned about their thoughts or behaviour to refrain from offending against children.[10]

This model is also eminently applicable to common cyber threats. Botnets are networks of compromised devices, whose processing power is hijacked to conduct attacks such as disabling websites by flooding them with traffic. A device can be compromised when an individual clicks on a suspicious link that downloads malicious software. Without their knowledge, that individual then facilitates attacks on other parts of society. Conversely, if the individual knows how to spot suspicious links and has antivirus software installed to stop and remove malicious software, they are able to prevent further attacks, or at least their part in them.

Or take ransomware, which locks devices until the user pays a ransom. Paying the ransom means *possibly* regaining access but certainly helps to fund organised crime, which has a detrimental impact on society. Governments in some rogue states reportedly benefit from the proceeds of ransomware, which means an individual paying a ransom in one country could indirectly facilitate human rights abuses in another. This was the case with the 2017 WannaCry attack, which infected devices in more than 150 countries and was attributed to 'cyber affiliates of the North Korean government'.[11] In something of a strange twist of fate, it led

[8] https://www.gresham.ac.uk/watch-now/fight-fake

[9] Baines, V. (2018) "Online Child Sexual Exploitation: Towards an Optimal International Response". *SSRN, August 29, 2018.* https://ssrn.com/abstract=3240998

[10] https://www.lucyfaithfull.org.uk/stop-it-now-helpline-campaign.htm

[11] The White House (2017) *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*. https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

to the declaration of a major incident in the UK's National Health Service.[12]

There are precedents also for applying the public health approach to wider societal issues. For instance, the World Health Organization includes violence prevention in its work, as one of the social determinants – social, physical, and economic conditions – that impact on health.[13] The approach comprises four main steps. These are:

1. Define and monitor the problem;
2. Identify risk and protective factors;
3. Develop and test prevention strategies;
4. Assure widespread adoption.

As the first step suggests, reliable data on the scale and nature of a problem is essential to determining the correct responses, and ensures that there is a solid evidence base for any measures developed and adopted. Just as COVID-19 cases, hospital admissions and excess deaths were continuously reported at the height of the coronavirus pandemic, so, too, we need to know how big a particular cyber problem is. This is easier said than done, because the data on cybercrime and cyber threats is so disparate. Law enforcement has data on reported crimes, technology providers have access to user reports, organisations of different types have logs of suspicious activity on their networks, anti-virus companies have data from scans of their customers' devices, and so on. European data protection legislation (GDPR) mandates reporting of data breaches to national authorities. But for the most part we need the data on cyber threats to be much more systematic and comprehensive in order for us to be able to decide whether we really do have a cyber pandemic, or whether that is just marketing hype.

Rehabilitating Viral Imagery

A public health approach to cybersecurity could legitimately adopt the language of community disease control, while at the same time giving agency to citizens. Public health communications need to be easily understood. So the technical jargon of cybersecurity must go. If we want target populations to take some kind of action, and even change their behaviour, we need to communicate clearly to them what they should do, and ensure that these actions are convenient and attractive. At the height of the COVID-19 pandemic, members of the public were not expected to have an advanced understanding of virology, immunology, or epidemiology. But we *were* expected to understand that hygiene and distancing measures help to control the spread of infection.

In the US, UK, and Commonwealth countries, generations of people became familiar with this concept through the 20th century slogan, "Coughs and sneezes spread diseases". While for some, the exhortation to use a handkerchief may smack of the nanny state, the phrase is so memorable that the World Health Organisation still uses it.[14] As Richard Massingham's 1945 public information film of the same name makes abundantly and joyously clear, it is possible to take a light-hearted attitude to serious issues, with the aim of engaging and activating the public.[15] But humour is very rarely deployed in public information about cyber threats.

A notable exception is Disney's *Ralph Breaks the Internet* (2018). Firmly targeting a family audience, it is an animated comedy in which lead characters Wreck-It Ralph and Vanellope von Schweetz enter the Internet via a Wi-Fi router. Online platforms are depicted as physical locations and algorithms as creatures; the overall presentation is both accessible and non-threatening. Pop-up advertiser J. B. Spamley guides Ralph into the Dark Net to source an 'insecurity virus' that will slow down a racing game with which Vanellope has become obsessed: the aim is to make the game boring so that she will want to leave. Ralph and Spamley descend in a lift to the Dark Net: a dank, dimly lit, green-tinged street, which houses the premises of Double Dan. Dan is a man-sized slug with more than a passing resemblance to *Star Wars*' Jabba the Hut and the voice of a cockney gangster. In a scene reminiscent of Monty Python's 'Dead Parrot' sketch and the purchase of the mogwai in *Gremlins*, the Dark Net is an exotic pet shop. The virus for sale bursts out of a toolbox. He is a

[12] Smart, W. (2018) *Lessons learned review of the WannaCry Ransomware Cyber Attack*. NHS England. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

[13] https://www.who.int/teams/social-determinants-of-health/violence-prevention

[14] https://www.who.int/europe/multi-media/item/coughs-and-sneezes-spread-diseases#

[15] https://www.nationalarchives.gov.uk/films/1945to1951/filmpage_cas.htm

mechanical, serpent-like monster, and his name is Arthur.

Arthur is by no means a cute pet, and his sudden explosion from the confines of his cage is surely intended to make a young audience jump. His dangerous potential is clearly signalled, but the comic setting, informal dialogue and cartoonish rendering refashion the Dark Net and cyber threats as intelligible to mass audiences. As depictions of cyber threats go, this is one of the most accessible and engaging. While its impact on the next generation of the world's adults remains to be seen, it nevertheless illustrates that what has become the default imagery for cybercrime prevention need not be the only, or even the most effective.

Borrowing from public health campaigns, we can instead consider how we might promote 'cyber hygiene', encourage people to 'practise safe cyber', and even keep our communities 'cyber clean and tidy'. It certainly sounds more achievable and empowering than messaging which depicts cybercrime as catastrophic, demonic, and inescapable. Meanwhile, applying a public health framework to cybersecurity enables us at a societal level systematically to identify problems, design targeted and holistic responses, designate those responsible for delivery, and justify the allocation of resources. The COVID-19 pandemic showed that many people *are* capable of taking measures to protect themselves and their communities. So why don't we entrust them to do the same with cybersecurity? We've tried fear, uncertainty, and doubt for the last three decades and it hasn't worked. Let's harness the lessons of the last few years to improve our cyber health. As a community, we stand a better chance of defeating digital viruses.

Resources

You can find some excellent videos online that introduce the discipline of Public Health. Among these:

- The website of King's College, London, has several videos on Global Health and Social Medicine - https://www.kcl.ac.uk/study-at-kings/ug/subjects/ghsm
- The YouTube channel of the US Centers for Disease Control and Prevention (CDC) contains a comprehensive lecture series - https://www.youtube.com/watch?v=-dmJSLNgjxo
- Dr Greg Martin is the Director of Ireland's Health Protection Surveillance Centre. His YouTube channel contains a large amount of engaging and informative content - https://www.youtube.com/@gregmartin

Further Reading

Baines, V. (2022) *Rhetoric of Insecurity: The Language of Danger, Fear and Safety in National and International Contexts*. London: Routledge.

EastWest Institute (2012) *The Internet Health Model for Cybersecurity*. https://www.eastwest.ngo/sites/default/files/ideas-files/Internethealth.pdf

Microsoft (2013) *Collective Defense: Applying Public Health Models to Internet Security*. https://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/collective_defense.pdf

Mulligan, D. K. & Schneider, F. B. (2011) "Doctrine for Cybersecurity". *Daedalus* 140.4: 70-92. https://direct.mit.edu/daed/article/140/4/70/26918/Doctrine-for-Cybersecurity

Parikka, J. (2016) *Digital Contagions: A Media Archaeology of Computer Viruses* (2nd edn). New York: Peter Lang

Rowe, B., Halpern, M. & Lentz, T. (2012) "Is a Public Health Framework the Cure for Cyber Security?". *CrossTalk*, *25*.6: 30-38. https://www.rti.org/publication/public-health-framework-cure-cyber-security/fulltext.pdf