Natural Language Engineering (2023), **29**, pp. 824–841
doi:10.1017/S1351324923000141

CAMBRIDGE UNIVERSITY PRESS

EMERGING TRENDS

Emerging trends: Risks 3.0 and proliferation of spyware to 50,000 cell phones

Kenneth Ward Church[1] and Raman Chandrasekar[2]

[1]Institute for Experiential AI, Northeastern University, San Jose, CA, USA and [2]Institute for Experiential AI, Northeastern University, Seattle, WA, USA
Corresponding author: Kenneth Ward Church; Email: k.church@northeastern.edu

(Received 10 April 2023; accepted 14 April 2023)

Abstract

Our last emerging trend article introduced Risks 1.0 (fairness and bias) and Risks 2.0 (addictive, dangerous, deadly, and insanely profitable). This article introduces Risks 3.0 (spyware and cyber weapons). Risks 3.0 are less profitable, but more destructive. We will summarize two recent books, *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy* and *This is How They Tell Me the World Ends: The Cyberweapons Arms Race*. The first book starts with a leak of 50,000 phone numbers, targeted by spyware named Pegasus. Pegasus uses a zero-click exploit to obtain root access to your phone, taking control of the microphone, camera, GPS, text messages, etc. The list of 50,000 numbers includes journalists, politicians, and academics, as well as their friends and family. Some of these people have been murdered. The second book describes the history of cyber weapons such as Stuxnet, which is described as crossing the Rubicon. In the short term, it sets back Iran's nuclear program for less than the cost of conventional weapons, but it did not take long for Iran to build the fourth-biggest cyber army in the world. As spyware continues to proliferate, we envision a future dystopia where everyone spies on everyone. Nothing will be safe from hacking: not your identity, or your secrets, or your passwords, or your bank accounts. When the endpoints (phones) have been compromised, technologies such as end-to-end encryption and multi-factor authentication offer a false sense of security; encryption and authentication are as pointless as closing the proverbial barn door after the fact. To address Risks 3.0, journalists are using the tools of their trade to raise awareness in the court of public opinion. We should do what we can to support them. This paper is a small step in that direction.

Keywords: Spyware; Pegasus; Phones; Responsible AI; Zero-click; Cybersecurity

1. Introduction

Our last emerging trend article Church *et al.* (2022) introduced Risks 1.0 and 2.0. Much of the literature on Responsible AI focuses on Risks 1.0 (fairness and bias), but we argued that there should also be more work on Risks 2.0 (addictive, dangerous, deadly, and insanely profitable). The use of machine learning to maximize engagement in social media has created a Frankenstein Monster that is exploiting human weaknesses with persuasive technology, the illusory truth effect, Pavlovian conditioning, and Skinner's intermittent variable reinforcement. Just as we cannot expect tobacco companies to sell fewer cigarettes and prioritize public health ahead of profits, so too, it may be asking too much of companies (and countries) to stop trafficking in misinformation given that it is so effective and so insanely profitable (at least in the short term).

This paper introduces a third case (Risks 3.0):

1. Risks 1.0: Biased and unfair (O'Neil 2016)

2. Risks 2.0: Addictive, dangerous, deadly, and insanely profitable (Fisher 2022; Bergen 2022):
3. Risks 3.0: Proliferation of military-grade spyware to 50,000 or more cell phones, targeting journalists, their friends and families, and many others (Richard and Rigaud 2023; Perlroth 2021).

There has been some interest in our field in deep fakes Li *et al.* (2020) that can be used for malicious purposes including a recent story on NPR.[a] The question is whether the problem is with the technology behind deep fakes or the malicious intent. To investigate this question, we thought it could be useful to survey technologies designed to cause harm: spyware, cyber weapons, etc.

Spyware is bringing back the nightmare of the Cold War:

These are exactly the methods that my parents experienced when they were living in Socialist Hungary. . . The methods that were used against me and the surveillance, this was really reminiscent of the Communist times. It was like being in a time machine, going back to my early youth, experiencing something that was going on in the 1980s. (Richard and Rigaud 2023, p. 140)

All three risks illustrate how technology in our field may have created a dystopian Frankenstein Monster that we no longer control.

One might dismiss these risks as a problem for someone else. One might mistakenly believe that:

1. Risks 1.0 are limited to women and minorities,
2. Risks 2.0 are limited to victims of riots (*involving a quarrel in a faraway country, between people of whom we know nothing*)[b] and
3. Risks 3.0 are limited to a few people that speak out too much about politics.

As Pastor Martin Niemöller famously said about taking action before it is too late:

First they came for the Communists
And I did not speak out
Because I was not a Communist
Then they came for the Socialists
And I did not speak out
Because I was not a Socialist
Then they came for the trade unionists
And I did not speak out
Because I was not a trade unionist
Then they came for the Jews
And I did not speak out
Because I was not a Jew
Then they came for me
And there was no one left
To speak out for me[c]

These risks, of course, have serious consequences for all of us. If we lose confidence in phones, computers, chips, banks, power grids,[d] and nuclear energy[e] (Perlroth 2021, p. 379) that could lead

[a] https://www.npr.org/2023/03/23/1165146797/it-takes-a-few-dollars-and-8-minutes-to-create-a-deepfake-and-thats-only-the-sta
[b] https://www.bbc.co.uk/archive/chamberlain-addresses-the-nation-on-his-negotiations-for-peace/zjrjgwx
[c] https://www.hmd.org.uk/resource/first-they-came-by-pastor-martin-niemoller/
[d] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[e] https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

to the end of the world, as noted by the title of Perlroth (2021): *This is How They Tell Me the World Ends*.

Our discussion of Risks 3.0 will summarize (Perlroth 2021; Richard and Rigaud 2023). The second book is titled *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy*. Pegasus is a spyware product sold by the NSO Group,[f] a company in Israel.

1.1 Connections between risks

There are many connections between these risks. It might seem that Risks 1.0 are more relevant to concerns of women and minorities, but many of these issues will come up in the following discussion of Risks 3.0. Gender comes up a number of times in Perlroth (2021):

> *Let's just say I stood out. For one, there are not many petite blondes in cybersecurity. To any woman who has ever complained about the ratio of females to males in tech, I say: try going to a hacking conference. With few exceptions, most hackers I met were men who showed very little interest in anything beyond code.* (p. 13)

In addition to gender, our discussion of Risks 3.0 will also touch on LGBTQ issues. Tim Cook, CEO of Apple, cares deeply about privacy,[g] partly because of his experience growing up in the closet in Alabama (Perlroth 2021, p. 239). Rachel Maddow, who wrote the introduction to the Pegasus book (Richard and Rigaud 2023), also cares about LGBTQ issues. She calls out NSO's reference to pedophiles as "a big company talking point the last few years" in her introduction to (Richard and Rigaud 2023, p. x). Pedophilia is a tired trope, often used by the right to attack people with unfounded/unspecified accusations of sexual "deviance" and "wokeness."

In our previous emerging trends article, we suggested "following the money" to deal with Risks 2.0. The incentives behind Risks 2.0 are closely linked to "insane profits." The business case for spyware is less compelling than for social media. The spyware business is less profitable and more destructive.

This paper, like our previous emerging trends article, will focus on implications for computer science. As computer scientists, we want to make it clear that we are not experts in journalism and other fields surveyed in these papers on risks. Nor are we entitled to a position on many of the questions raised in the work cited here. Our goals are more modest than that. We want to survey criticisms that are out there and suggest that our field should work on responses.

The books mentioned above are written by journalists. Nicole Perlroth covered cybersecurity and digital espionage for The New York Times.[h] Laurent Richard and Sandrine Rigaud work for Forbidden Stories[i] in France. They are using the tools of their trade to make a compelling case in the court of public opinion, raising awareness of risks that need to be taken more seriously. This genie is not going back into the bottle. We will have to deal with spyware sooner or later. COVID taught us how important it is to deal with contagious viruses before they spread out of control.

1.2 Agenda

Section 2 will sketch out a future dystopia where spyware proliferates well beyond a few rich countries. Everyone will get hacked by everyone.

Section 2.1 will discuss how we got into this mess. Much of the history goes back to efforts by the American government to fight terrorism. These efforts may have been well-intentioned, but

[f] https://www.nsogroup.com/
[g] https://www.youtube.com/watch?v=rQebmygKq7A
[h] https://www.nytimes.com/by/nicole-perlroth
[i] https://forbiddenstories.org/our-team/

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

there may be long-term unintended consequences, leading to a loss of confidence in all things digital, elections, banking, and the economy. Russia pushed for a treaty banning computer warfare, but their overture was rejected by the Americans, as discussed in Section 2.3.

Section 3 summarizes the Pegasus Book (Richard and Rigaud 2023). The latest version of Pegasus uses a highly effective zero-click exploit that infects a phone without the victim clicking on anything. The scale is "eye-popping"; the Pegasus book starts with a leak of 50,000 targeted phone numbers. Many people are upset about Risks 3.0; Section 4 will focus on three famous/infamous celebrities: Rachel Maddow, Ronan Farrow, and Edward Snowden.

Spyware is designed to be hard to detect, but it is hard to keep it a secret when it is so pervasive, as discussed in Section 5. Section 6 will discuss constructive suggestions. One of the more promising ways forward is to make the case in the court of public opinion. Journalists are using the tools of their trade to do exactly that. In addition to non-technical suggestions, we will mention a few technical opportunities for people in our field.

2. Spyware and future dystopia

In the past, spyware was mostly used by countries to spy on one another, but it is proliferating beyond that. Perlroth wrote a "news analysis" piece in June 2021, a month before many of the Pegasus stories were published, with the provocative title:[j]

Are we waiting for everyone to get hacked?

and an even more provocative subtitle:

It's been almost a decade since Leon Panetta, then the secretary of defense, warned of an impending "Cyber Pearl Harbor." He didn't want to be right.

The ending is sobering:

Mr. Panetta. . . has his own simple solution for staying safe—and specifically making sure his internet-connected Lexus isn't hacked. A few years ago, he fixed up his dad's old 1951 Chevy truck, and that is what he uses to get around.

When he does drive the Lexus, he has careful instructions for his passenger: "I tell my wife, 'Now be careful what you say.'"

To protect users, technology companies such as Google have been tracking the activities of commercial spyware vendors. They are detecting proliferation[k] by new vendors such as Variston.[l,m]

Spyware is used for many purposes. In the past, the technology enabled countries to spy on one another, steal money,[n] and settle scores. As the technology proliferates, organized crime and petty thieves will do much of the same to millions of innocent victims. Spyware will be cheaper and more effective than divorce lawyers, SLAPP suits,[o] and most legitimate and illegitimate ways of getting "even."[p]

[j] https://www.nytimes.com/2021/06/05/business/leon-panetta-cyber-attacks.html
[k] https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/
[l] https://techcrunch.com/2023/03/29/hackers-variston-spyware-uae-google/
[m] https://variston.net/
[n] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a
[o] https://www.law.cornell.edu/wex/slapp_suit
[p] https://www.findlaw.com/criminal/criminal-charges/revenge-porn-laws-by-state.html

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

We live in a target-rich environment. The bad guys have already broken into banks, the power grid (Perlroth 2021, chapter 19), and nuclear plants (Perlroth 2021, p. 379). Can you trust the chips in your car? Or your refrigerator? Or the traffic lights?[q] Maybe smartphones and smart cities aren't so smart, when it is so easy to hack them. Is the Internet of things creating a better world, or a world with more targets?

Trust is key to banking,[r] and all things digital. If spyware leads to a loss in confidence, the economy will suffer. When spyware becomes pervasive, nothing will be safe: not your identity, or your secrets, or your passwords, or your bank accounts.[s] When the endpoints (phones) have been compromised, technologies such as end-to-end encryption and multi-factor authentication offer a false sense of security. Once the endpoints have been compromised, encryption and authentication are as pointless as closing the proverbial barn door after the fact.

2.1 How did we get into this mess?

As governments were fighting the war on terrorism, they undermined confidence in technology. That is, when the government breaks into a phone, even for legitimate reasons, there is a risk that the government's actions will help the bad guys figure out how to break into phones for less legitimate reasons.

In addition, some apps have become extremely popular. Unfortunately, this popularity leads to monocultures. Biodiversity is important in nature to defend against viruses and other risks.

1. Good enough to sell → (risky) monocultures.
2. Trust needs to be a top priority. Governments prioritized the war on terrorism above trust in all things digital.

2.1.1 Good enough to sell → monocultures

Good enough to sell is good enough for some purposes, but not for others. The first author was once in Microsoft's executive briefing room when a military customer made it clear that Microsoft products offered better value for money than defense contractors. The military knew that "mil spec" was not working for them, but they hoped to convince Microsoft to make their products more robust. We are betting the country and the future of the world on consumer-grade products that were never designed to be good enough for those use cases. We should not depend too much on products that were never designed to be that dependable.

The good-enough-to-sell policy has produced monocultures. Pegasus targets popular apps like WhatsApp[t] because they are popular. Technology would be less exposed to threats such as Pegasus if there was more "app diversity." App diversity is important for the same reasons that biodiversity is important in nature.

2.1.2 Trust needs to be a top priority

We have been putting all our eggs in one basket. That may be convenient, but it is also risky. For example, two-factor authentication used to run on stand-alone fobs that are less exposed to hacking. We need more compartmentalization and defense in depth (DiD).[u] Moving two-factor authentication back to stand-alone fobs would improve security (and confidence in the system). The keys to your bank account should be kept in a safe[v] off the grid, with no connection to the

[q] https://archive.nytimes.com/bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers/
[r] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/12/statement-from-president-joe-biden-on-actions-to-strengthen-confidence-in-the-banking-system/
[s] https://therecord.media/sec-cyber-incident-reporting-rules-finance
[t] https://www.reuters.com/legal/us-supreme-court-lets-metas-whatsapp-pursue-pegasus-spyware-suit-2023-01-09/
[u] https://csrc.nist.gov/glossary/term/defense_in_depth
[v] https://www.nytimes.com/wirecutter/reviews/best-fireproof-document-safe/

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

Internet (or anything else). The keys to your most important secrets should not be commingled with other stuff on your phone (unless there is a super-compelling reason to do so).

Ken Thompson's Turing Award speech on trust (Thompson 1984) emphasized the size of the attack surface. He argued that it should be kept small enough that it can be verified by a single person:

You can't trust code that you did not totally create yourself. . . . No amount of source-level verification or scrutiny will protect you from using untrusted code. . . .A well-installed microcode bug will be almost impossible to detect. . . .

Thompson also argued that violations of trust should have serious consequences in the court of public opinion:

. . . The act of breaking into a computer system has to have the same social stigma as breaking into a neighbor's house. It should not matter that the neighbor's door is unlocked. The press must learn that misguided use of a computer is no more amazing than drunk driving of an automobile.

Thompson was objecting to hacking by teenagers, which was a serious problem in 1980s. It is a shame that since then the US government has become one of the worst offenders, especially since their recklessness is protected by legal immunity.

We should view our phones like the mail. We have confidence in the mail system, not because it is designed to be hack proof, but because hacking the mail is a federal offense. So too, hacking phones ought to be taken seriously. Unfortunately, hacking is in a gray area.

Tim Cook, CEO of Apple, has consistently defended privacy (over other concerns such as national security):

At the closed-door meeting, Obama made the case for a balanced approach to privacy and national security. Cook listened intently, and when it came time to speak, he shared what he'd heard from Apple's customers abroad. There was now a deep suspicion of America's technology companies, he told the president. America had lost its halo on civil liberties, and it might be decades before it ever earned it back. Leaving anything open to surveillance was, in his mind, a civil liberties nightmare, not to mention bad business. People had a basic right to privacy, and if American companies couldn't protect them, they would take their business overseas. Cook was putting the government on notice: Apple was going to encrypt everything. (Perlroth 2021, p. 240)

The government should be held liable for the consequences of its actions in the court of public opinion, if not in a legal court. When the government breaks into a phone, it creates a loss in confidence that has serious consequences for billions of users. If we lose confidence in all things digital, elections, banking, and the future of the world, those consequences far outweigh the benefits of solving a particular crime. Unfortunately, the government is rarely held liable for the consequences of its actions, even when there is little to show for their recklessness.

For example, after a 2015 shooting in San Bernardino, CA, the FBI asked Apple to break into the iPhone of a person of interest. When Apple refused to cooperate, fearing consequences for billions of their customers, the FBI proceeded anyways and found another way to break into the iPhone. In the end, the FBI's effort risked much and produced little:

In the end, not much happened as a result of the effort. The FBI reportedly didn't get any useful information from the phone[w]

There are few incentives for the FBI to be concerned about the downsides of breaking into that iPhone.

[w]https://www.theverge.com/2021/4/14/22383957/fbi-san-bernadino-iphone-hack-shooting-investigation

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

2.2 Asymmetric conflict

As mentioned above, much of the spyware technology was originally developed by bigger countries to spy on smaller countries, but in retrospect, the NOBUS (nobody but us) policy[x] turned out to be short-sighted and deeply flawed.

Consider Stuxnet,[y] an exploit that caused substantial damage to Iran's nuclear program. In the short term, Stuxnet was cheaper than conventional weapons, but it did not take long for Iran to catch up and use the technology against Saudi Arabia and the United States:

The worm had crossed the Rubicon from defensive espionage to offensive cyberweapon, and in just a few years, it would come boomeranging back on us. (Perlroth 2021, p. 131)

While Stuxnet may have been viewed as a relatively cheap method to address the nuclear threat from Iran, the consequences may have turned out to be more expensive than originally thought. Leon Panetta made the comparison with Pearl Harbor [underlining added]:

"We were astounded that Iran could develop that kind of sophisticated virus," Leon Panetta, then secretary of defense, told me later. "What it told us was that they were much further along in their capability than we gave them credit for. We were dealing with a virus that could have just as easily been used against our own infrastructure. It was a weapon that could create as much havoc and destruction as 9/11 or Pearl Harbor." (Perlroth 2021, p. 268)

The connectivity of the Internet is both a blessing as well as a curse; from the perspective of information security, connectivity should be replaced by compartmentalization and defense in depth [underlining added]:

By the time the NSA's exploits boomeranged back on American towns, cities, hospitals, and universities. . . For decades the United States had conducted cyberwarfare in stealth, without any meaningful consideration for what might happen when those same attacks, zero-day exploits, and surveillance capabilities circled back on us. And in the decade after Stuxnet, invisible armies had lined up at our gates; many had seeped inside our machines, our political process, and our grid already, waiting for their own impetus to pull the trigger. For all the internet's promise of efficiency and social connectivity, it was now a ticking time bomb. (Perlroth 2021, p. 346)

There was a time when might (larger budgets) made right, but that is no longer the case:

The United States still had the biggest offensive cyber budgets, but compared to conventional weapons, exploits were cheap. Foreign governments were now willing to match American prices for the best zero-days and cyberweaponry. The Middle East's oil-rich monarchies would pay just about anything to monitor their critics. And in Iran and North Korea, which could never match the United States in conventional warfare, leaders saw cyber as their last hope of leveling the playing field. If the NSOs, Zerodiums, and Hacking Teams of the world wouldn't sell them their wares, well, they could just hop on a plane to Buenos Aires. (Perlroth 2021, p. 259)

In response to a suggestion that our side was good and their side was bad, Arce, a hacker in Argentina, responded to Nicole Perlroth with:

"You need to dispose of your view, Nicole," Arce told me. "In Argentina, who is good? Who is bad? The last time I checked, the country that bombed another country into oblivion wasn't China or Iran." (Perlroth 2021, p. 265)

[x] https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/

[y] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

2.3 What goes around, comes around

The barrier to entry was so low that for the cost of three F-35 stealth bombers, Iran. . . built a world-class cyber army. But four short years later [after Stuxnet], *Iran had not only recovered its uranium but also* [installed more uranium centrifuges] *. . . And now Tehran claimed to have the "fourth-biggest cyber army in the world."* (Perlroth 2021, p. 270)

As for Russia, China, and others, it is hard to complain about them, given what we in the US have done.

"It was the old people-in-glass-houses problem," a senior Obama official told me. (Perlroth 2021, p. 280)

Google worked hard to fight a Chinese hack and objected so strongly that they were kicked out of the Chinese market. But soon after that, they discovered that they were also hacked by the United States:

Behind the scenes, Google security engineers were more forthright. "Fuck these guys," a Google security engineer named Brandon Downey wrote in a post to his personal Google Plus page. Downey and hundreds of other Google engineers had just dedicated the previous three years to keeping China from hacking its customers, only to find out they'd been had by their own government. (Perlroth 2021, p. 235)

Russia pushed for a treaty banning computer warfare, but Washington rejected the overture [underlining added]:

Not long after Stuxnet escaped, Russian officials–dismayed by what the Americans and Israelis had pulled off in the cyber realm–began agitating for an international cyberweapons ban. . .. Russia's attack surface was vast, and only getting bigger. Russian Grids PJSC, the state-controlled utility, ran 2.35 million kilometers of transmission lines and 507,000 substations around the country. . . Following on the discovery of Stuxnet, Russian officials feared they made for an obvious American target. In a speech in 2012, Russia's minister of telecommunications pushed for an international treaty banning computer warfare, while Russian officials back-channeled with their American counterparts to come up with a bilateral ban. But Washington dismissed Moscow's bids, believing them to be a Russian diplomatic ploy to neuter the U.S. lead in cyberwarfare. With no treaty in sight, it appeared that Russia was now implanting itself in the American grid–and at an alarming pace. Over the next year and a half, Russian hackers made their way inside more than a thousand companies, in more than eighty-four countries, the vast majority of them American. (Perlroth 2021, pp. 286–287)

When the treaty failed, Russia invested in cyber warfare:[z]

The trove offers a rare window into the secret corporate dealings of Russia's military and spy agencies, including work for the notorious government hacking group Sandworm. U.S. officials have accused Sandworm of twice causing power blackouts in Ukraine, disrupting the Opening Ceremonies of the 2018 Winter Olympics and launching NotPetya, the most economically destructive malware in history.

The Kremlin has become so aware of the risks that they reportedly told Russian officials to throw away their iPhones.[aa]

[z] https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/
[aa] https://www.kommersant.ru/doc/5886759

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

To summarize, how did we get into this mess, and who is to blame? Unfortunately, the answer seems all too clear. We did it to ourselves. We created a Frankenstein monster while attempting to fight terrorism. The effort to *get left of boom* (Perlroth 2021, p. 290), military jargon for attempts to stop a bomb before it detonates, may have been well-intentioned. But these efforts may have long-term consequences, leading to a loss of confidence in all things digital, elections, banking, the economy, and the world as we know it. As bad as terrorism is, it is not the end of the world.

3. Pegasus

Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy (Richard and Rigaud 2023) (henceforth "The Pegasus Book") describes one of the more successful spyware products, Pegasus,[ab] a program sold by NSO,[ac] that can take control of a phone and spy on the victim with their own camera, microphone, GPS, etc. Once Pegasus has obtained root access, it can exfiltrate text messages, contacts, and anything else of value on the phone, or within range of the camera, microphone, wifi, bluetooth, etc. We complain about millions of cameras in China, but who needs a camera on a street corner when anyone can do whatever they want with the phone in your pocket.[ad]

3.1 Zero-click exploit

At first, Pegasus made use of phishing attacks and social engineering, but more recent "new and improved" versions no longer require the victim to click on anything. Pegasus's "zero-click" exploit is so effective that NSO gained a dominant position in the spyware market:

> *One year later, Hacking Team* [a competitor in the spyware business][ae] *was still unable to match NSO's zero-click feature, and it was hemorrhaging customers left and right.* (Perlroth 2021, p. 180)

After the zero-click upgrade, it is no longer necessary for Pegasus to leave as much evidence on the infected phone:

> *"[The malware] is not actually stored on the phone," . . . "So if you reboot the phone or your battery runs out, the infection cleans up. But [the Pegasus end users] don't care because they were just going to reattack you again at the next opportunity. And that's just pretty automatic. They can decide on Tuesday, we'll just get all the SMS messages, and then we'll get them again on Thursday. . . there is no condition that stops them from being successful. As long as they have the exploit working, they can exploit you like five times a day and just upload whatever they want in that particular moment."* (Richard and Rigaud 2023, p. 206)

3.2 Leak of 50,000 targeted phone numbers

The Pegasus book describes a year-long investigation into Pegasus by Forbidden Stories,[af] a small team of journalists in France[ag] who worked with 60 news organizations and more than 150 journalists from 49 countries and five continents. The book begins with a call from a source on August 5, 2020 and ends with publications of their findings in many papers around the world in July of

[ab] https://en.wikipedia.org/wiki/Pegasus_(spyware)#
[ac] https://en.wikipedia.org/wiki/NSO_Group
[ad] https://www.gocomics.com/pearlsbeforeswine/2023/03/07
[ae] https://en.wikipedia.org/wiki/Hacking_Team
[af] https://forbiddenstories.org/case/the-pegasus-project/
[ag] https://forbiddenstories.org/our-team/

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

2021. While this is not the first reporting on Pegasus,[ah,ai] what makes the Pegasus project such a big story is: 50,000.

The story begins with a leak of 50,000 phone numbers that have been targeted by Pegasus. 50,000 is a huge number. Pegasus appears to have targeted more phone numbers in four years than four decades of FISA[aj] warrants.[ak] This may be an unfair comparison since FISA warrants may include more than one phone number, and FISA warrants are not required for foreigners in foreign lands,[al] and FISA rules are not always followed.[am] Nevertheless, 50,000 is a huge number.

The size of the list is not only unusually large (50,000), but the quality is also unusually high. According to Claudio Guarnieri,[an] a key figure in the Pegasus book, who is not one to "overhype":

> *"The leads that the data is giving us are extraordinary because the amount of success we're having with the forensics is, to me, unprecedented. And let me tell you that I've been working on the surveillance industry for a decade. I have probably checked hundreds of computers and phones in these years, and if I had a zero-point-five-percent success before this, it would have been good. And now I think we're close to eighty percent. So to me that's a sign that this is pretty strong." This was the boldest assertion I had ever heard Claudio make about his confidence in the data and in the forensics. At that point, he even allowed himself a quick chuckle, as if he might have surprised himself.* (Richard and Rigaud 2023, pp. 207–208)

NSO objects to the Pegasus book[ao] and argues that Pegasus has saved lives,[ap] but it is clear that Pegasus has proliferated well beyond criminals and threats to national security [underlining added]:[aq]

> *The list* [of 50,000 targeted phone numbers] *no doubt contained hundreds of cell phone numbers of authentic drug lords, terrorists, criminals, and national security threats–the sort of malefactors NSO spokespeople claimed Pegasus was designed to thwart. But. . . the range of targets selected for attack was eye-popping. . . it turned out that many belonged to academics, human rights defenders, political dissidents, government officials, diplomats, businessmen, and high-ranking military officers. . . The group with the largest number of targets. . . was journalists.* (Richard and Rigaud 2023, p. 8)

[ah] https://www.youtube.com/watch?v=Y6e_ctKqSqM

[ai] https://www.blackhat.com/eu-16/briefings/schedule/#mobile-espionage-in-the-wild-pegasus-and-nation-state-level-attacks-5127

[aj] https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

[ak] https://web.archive.org/web/20180427170434/https://epic.org/privacy/surveillance/fisa/stats/default.html

[al] "NSO always claimed that Pegasus could not be used on a cell phone with a US number (any number with a plus-1 country code)," according to Richard and Rigaud (2023), p. 19, though FISA rules probably do not apply to foreign companies and they do not define foreigners by the syntax of the phone number, partly because mobile phones are mobile, and therefore, one cannot depend on phone numbers to determine jurisdiction. Moreover, even before mobile phones, plus-1 country codes include many places outside the US such as Canada and much of the Caribbean, and exclude many US places such as military bases and embassies around the world. FISA rules require government agencies in the US to obtain a warrant from a judge to target anyone in the US or a US person anywhere in the world.

[am] https://en.wikipedia.org/wiki/NSA_warrantless_surveillance_(2001-2007)#

[an] https://limn.it/researchers/guarnieri/

[ao] https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/

[ap] https://www.haaretz.com/israel-news/tech-news/2021-08-15/ty-article/.premium/after-spyware-scandal-israeli-nso-https://www.haaretz.com/israel-news/tech-news/2021-08-15/ty-article/.premium/after-spyware-scandal-israeli-nso-

[aq] "Recent hacking of 9 US diplomats shatter all claims by NSO that. . .help governments fight terrorism and crime. Sypware is a threat to human rights and diplomacy. . . It is a threat to world peace. . . and now that this threat is closer to home, we hope that it tips the Biden Administration and the European Union to sanction NSO Group and ban the use of this technology" https://youtu.be/Q_sR7phqbyI?t=190.

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

3.3 Scandals everywhere, all at once

Journalists are especially outraged by attacks on journalists, but there are plenty of other scandals around the world. For example, evidence of infections was found on politicians in France, Mexico, Spain[ar,as,at] (Catalonia),[au] India,[av] and many other places. After a dozen US State Department employees were hacked, Biden issued an executive order banning US government agencies from using spyware that is deemed a threat to US national security or are implicated in human rights abuses.[aw]

As for Macron and Rugy, two politicians in France,[ax] their phones were probably hacked by Morocco, a former colony of France. As mentioned above, spyware used to favor big countries with big budgets, but these days, spyware favors underdogs with less to lose and more to gain.

Many politicians are hacked by their opponents as described in footnote [ab] and elsewhere[ay,az,ba] in scandals that are reminiscent of Watergate,[bb] as reported in the news in India.[bc] When Nixon hacked the Democrats, the scandal led to his resignation. But these days, there are more hacks, and fewer consequences (at least for the hackers).

Unfortunately, the consequences for the targets of the hacks can be severe.[bd] Pegasus probably played a role in the murder of journalist Jamal Khashoggi[be,bf,bg,bh] and many others.[bi,bj]

4. Outrage from three famous/infamous celebrities

4.1 Rachel Maddow's outrage

The introduction to the Pegasus book was written (and narrated in the audio version) by Rachel Maddow. Her outrage comes across even more clearly in her narration (as well as her comments on her television show).[bk] She leads with a teaser suggesting that all is not right [underlining added throughout this section]:

The call [on August 5, 2020] *appeared urgent, in that it was coming. . .from somebody in senior management at the NSO Group. . . . This was a delicate high-wire act, ethically speaking,*

[ar] https://www.ft.com/content/e24bc019-7619-4f87-8518-cfea0f37210a
[as] https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware
[at] https://www.aljazeera.com/news/2022/5/2/spain-detects-pegasus-spyware-on-pm-defence-ministers-phones
[au] https://www.politico.eu/article/pegasus-spyware-targets-top-catalan-politicians-and-activists/
[av] https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance
[aw] https://www.cnn.com/2023/03/27/politics/us-government-bans-spyware/index.html
[ax] https://youtu.be/xYMWTXIkANM
[ay] https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy
[az] https://www.reuters.com/world/americas/mexico-president-says-government-does-not-spy-after-pegasus-spyware-https://www.reuters.com/world/americas/mexico-president-says-government-does-not-spy-after-pegasus-spyware-
[ba] https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0
[bb] https://www.senate.gov/about/powers-procedures/investigations/watergate.htm
[bc] This video, https://www.youtube.com/watch?v=x3bl4dggpAU, leads with a reference to Watergate and then follows that up with a defense of the government in India. There are relatively few videos on YouTube that defend governments, but this is one of the few exceptions.
[bd] https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-scandal-khadija-ismayilova-documentary-excerpt/
[be] https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/
[bf] https://www.pbs.org/wgbh/frontline/article/how-nso-group-pegasus-spyware-found-jamal-khashoggi-fiancee-phone/
[bg] https://www.theguardian.com/world/2022/sep/22/jamal-khashoggis-wife-to-sue-nso-group-over-pegasus-spyware
[bh] https://podcasts.apple.com/us/podcast/shoot-the-messenger-espionage-murder-pegasus-spyware/id1661177850
[bi] https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto
[bj] https://www.lemonde.fr/en/international/article/2022/10/04/new-victims-of-pegasus-spyware-in-mexico-despite-government-promises_5999023_4.html
[bk] https://www.youtube.com/watch?v=mQfLxaxLE3Q

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

because NSO's signature product. . . Pegasus was a remarkable and remarkably unregulated tool–extraordinarily lucrative to the company (NSO grossed around $250 million that year [2020]*) and dangerously seductive to its clients. . .*

She is deeply convinced that Pegasus might go beyond legitimate targets:

NSO insists its software and support services are licensed to sovereign states only, to be used for law enforcement and intelligence purposes. They insist that's true, because–my God–imagine if it weren't.

Given the size of the market, it is hard to imagine how NSO's claims could be enforced. She calls out the discussion of pedophiles as a tired trope, popular with the right:

The cybersurveillance system the company created and continually updates and upgrades for its sixty-plus clients in more than forty different countries has made the world a much safer place, says NSO. Tens of thousands of lives have been saved, they say, because terrorists, criminals, and pedophiles (pedophiles is a big company talking point the last few years) can be spied on and stopped before they act.

She knows that many journalists have been targeted by Pegasus, and some of them were murdered, as discussed in Section 3.3:

The insidious power of a Pegasus infection was that it was completely invisible to the victim–you'd have no way to know the baddies were reading your texts and emails and listening in on your calls and even your in-person meetings until they used their ability to track your exact location to send the men with guns to meet you.

There are many other examples of innocent victims including a princess involved in a messy divorce:

the spying on the princess and her lawyer didn't really shake out into public view until more than a year later, and only then because it was part of the child custody proceedings. . . A FUNNY THING happened on the way to that divorce court. . . Because right around the time [of the leak mentioned above], *a very brave source offered two journalists from Paris* [the authors of the Pegasus book] . . . *access to a remarkable piece of leaked data. . .. Fifty thousand. . .*

Many people are concerned about the number of phone numbers. She is not alone:

If you believe your privacy is being secured by encryption, please read this book. . . If they could do it for fifty thousand, doesn't that mean they could do it for five hundred thousand? Five million? Fifty million? Where is the limit, and who is going to draw that line? Who is going to deliver us from this worldwide Orwellian nightmare? . . . Where did you say your phone is right now?

The story continues to unfold. At the end of Maddow's show (see footnote[bk]), she mentions a ban by the US government[bl] as well as a lawsuit involving the US Supreme Court.[bm]

There were many news stories on Pegasus when the Pegasus Project published their findings in July 2021, but Pegasus and spyware continue to be discussed in the news, including some recent articles.[bn,bo,bp]

[bl] https://www.theverge.com/2021/11/3/22761565/nso-group-pegasus-spyware-entity-list-us-government-human-rights

[bm] https://www.nbcnews.com/politics/supreme-court/supreme-court-allows-whatsapp-lawsuit-pegasus-spyware-move-forward-rcna64141

[bn] https://www.nytimes.com/2023/03/15/world/americas/interpreter-pegasus-spyware-mexico.html

[bo] https://www.nytimes.com/2023/03/27/us/politics/biden-spyware-executive-order.html

[bp] https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

4.2 Ronan Farrow's outrage

Rachel Maddow is not the only celebrity to be outraged by Pegasus. Ronan Farrow published an article in the New Yorker[bq] and a podcast.[br] To promote that work, he gave an interview to Estrin on NPR:[bs]

FARROW: . . .*this kind of technology is not going away*. . . *These companies are going to go on and*. . . *thrive.*

ESTRIN: *And it's not just Israeli companies. You describe Chinese companies doing the same thing.*

FARROW: *Yes. China and Russia both provide this tech to other states*. . . *The United States does the same, by the way. So this is a genie that is not going back in the bottle any time soon.*

Farrow continues with a comparison to the regulation of traditional arms. Spyware is "a powerful weapon that is not being restricted in the way that chemical weapons or nuclear weapons are."

More recently, Ronan appeared on an amazing interdisciplinary panel (with remarkably few views on YouTube). The journalists on the panel, Ronan Farrow and Carlos Dada (El Faro), made a strong case, though many of those arguments can be found elsewhere. The lawyer, Carrie DeCell,[bt] mentioned a number of law suits against NSO by companies such as Apple,[bu] Google,[bv] Facebook,[bw] and others including members of the panel. Unfortunately, these cases will take a few years. In the meantime, DeCell encouraged journalists and the tech companies to combat this threat in the court of public opinion. The moderator underscored her comment with: "it is very rare that journalists are suing the same company that Apple and Meta are. . . this is something new. . ."[bx]

4.3 Edward Snowden's outrage

As mentioned above, Rachel Maddow is not the only one concerned by fifty thousand:

Edward Snowden is not easily shocked by stories about the spread of cybersurveillance, but he seemed taken aback. He was silent for a couple of seconds, while the number sank it. "Fifty thousand," he said. "Wow." (Richard and Rigaud 2023, pp. 269–270)

The discussion continues on pp. 270–271:

A company like [NSO] really shouldn't exist. . . *These are devices that exist in every context, on every desk, every home, all over the world, and we are dependent. We cannot work, we cannot communicate, we cannot trade, we cannot go about our lives in a normal expected way today without using these*. . . *The only thing that the NSO group does, their only product is trying to discover weaknesses in these devices that we all rely on and then sell them commercially*. . . *There's no limitation.*

[bq] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

[br] https://www.newyorker.com/podcast/politics-and-more/ronan-farrow-on-the-threat-of-modern-spyware

[bs] https://www.npr.org/2022/04/21/1094119453/ronan-farrow-on-investigating-the-world-s-most-notorious-spyware-company-nso-gro

[bt] She has given more recent interviews on Democracy Now! https://www.youtube.com/watch?v=GudI5b0DpQw.

[bu] https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html

[bv] https://www.middleeasteye.net/news/microsoft-google-join-facebook-legal-israel-nso-group

[bw] https://www.reuters.com/technology/facebook-can-pursue-malware-lawsuit-against-israels-nso-group-us-appeals-court-2021-11-08/

[bx] https://youtu.be/lM7JI4hcMeI?t=2583

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

There's only Israel pinky promising that they're going to have their Ministry of Defense or whatever review the export license.

Snowden suggested a constructive suggestion that will be discussed in Section 6:

Just ten minutes into the call, Snowden was on a roll. The fix, as he saw it, was some kind of global regulation to bring the cybersurveillance industry to heel. Maybe the EU would be moved, finally, to act. NSO is "not trying to save the world," he continued. "They're not trying to do anybody any good. They're trying to make money despite their public claims to the contrary. When you create the means of infection, and you start passing them off to the highest bidder, as the NSO Group has done and is doing and will do tomorrow–if nothing changes, you're creating, you are guaranteeing that the world will be less safe tomorrow than it is today."

The call ended with an offer of support:

Before he signed off, Snowden told Paul he would be happy to assist the Pegasus Project any way he could. "If you guys want me to help, like, just announce it," Snowden said, "because this is a story."

When the story came out in July 2021, Snowden tweeted:[by]

Stop what you're doing and read this. This leak is just going to be the story of the year. (Richard and Rigaud 2023, p. 291)

Snowden reiterated many of these comments in an interview in the Guardian[bz] and went on to say, "but the NSO Group is only one company of many, and if one company smells this bad, what's happening with all the others." In response to a question, "In the past you have called smartphones a spy in your pocket. Do you think this confirms that?" Snowden replied,

I think this is actually worse. . . they are. . . taking control of that phone fully and turning it against the people that bought and paid for it. . . but no longer truly own it. . . If they found a way to hack one iPhone, they found a way to hack all of them and they are doing that and they are selling that.

If you don't do anything to stop the sale of this technology, it's not just going to be 50,000 targets. It's going to be 50 million targets, and it's going to happen much more quickly than any of us expect.[ca]

5. Stealth, plausible deniability and deterrence

In World War II, when the Allies broke the German and Japanese codes, they were very careful to keep that a secret. Spyware is also often designed to be invisible, though it is hard to keep anything a secret when deployed at scale. It is inevitable that Pegasus will be caught when it is running on 50,000 phones. Moreover, the gray market for zero-day exploits suggests there is plenty of supply.[cb,cc] Phones have such a large attack surface that there are plenty more bugs (exploits) to be found.

Given that reality, the strategy has moved from stealth to plausible deniability. NSO argues that they design Pegasus to be used by legitimate governments on legitimate targets for legitimate

[by] https://twitter.com/Snowden/status/1416797153524174854
[bz] https://www.youtube.com/watch?v=I5WjTTi67BE
[ca] https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations
[cb] https://en.wikipedia.org/wiki/Market_for_zero-day_exploits
[cc] https://www.lifars.com/2021/01/current-state-of-zero-day-exploit-market/

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

purposes. Any misuse of their product is a violation of the terms of service. To the extent that there may be misuse, it is someone else's fault:

NSO is a technology company. We do not operate the system, nor do we have access to the data of our customers[cd]

This argument does not appear to be a winning argument:[ce]

But software coders and engineers in Tel Aviv were swapping stories of NSO employees going sheepishly silent when asked to recount their workweek at Shabbat family dinners on Friday night.

Sales of Pegasus slowed to a trickle, and Moody's pronounced the company in danger of defaulting on its debt. There was some doubt that NSO could make its November 2021 payroll. (Richard and Rigaud 2023, p. 300)

When BRG insisted that "the plan was fraught with risk," according to the Financial Times, "[Shalev] quipped back that it was risky to miss a debt payment too."[cf] (Richard and Rigaud 2023, p. 300)

The Financial Times has continued to report on NSO's difficulties. Their stock may be worthless.[cg]

A third strategy is deterrence. Spyware can be effective if the public believes that it is effective. Consider cameras in China. Many of these cameras are designed to be seen. If they wanted to spy on you without being seen, they could easily do that. The highly visible cameras are intended to deter crime by convincing the public that the technology is more effective than it is.

So too, perhaps the point of the NSO Group, at least from the perspective of the Israeli government, is to convince the world that their spyware is more effective than it is. While the use of spyware as a deterrent may be an effective strategy for defending against certain threats to national security, the benefits to one country may not be worth the cost of undermining worldwide confidence in all things digital.

6. Constructive suggestions

What can we do about Risks 3.0? Many suggestions have been mentioned above:

1. Raising awareness in the court of public opinion (Section 4)
2. Law suits (footnote[BM])
3. Diplomacy (as discussed in Section 2.3, Russia's request for a treaty was rejected because the U.S. believed it had a lead in cyberwarfare)

6.1 Non-technical remedies

Some suggestions are technical and some are not. Some are more likely to succeed, and some are less likely to succeed. We need to make more progress in the court of public opinion before we can hope to make much progress on the other suggestions.

[cd] https://www.nsogroup.com/Newses/enough-is-enough/
[ce] https://forbiddenstories.org/the-rise-and-fall-of-nso-group/
[cf] https://www.ft.com/content/5ef90e5f-1220-4ed6-a650-985272eb0334
[cg] https://www.ft.com/content/057cece3-eb81-42b8-9a27-e295c61e76b3

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

As for diplomacy, Brad Smith of Microsoft made a passionate case for a "Digital Geneva Convention" in 2017,[ch,ci] but "there is only little hope that such global treaty is likely to be created any time soon" (Koloßa 2019; Jeutner 2019). Diplomacy and legal systems cannot keep up with technology's ability to move fast and break things. Fortunately, the court of public opinion is faster because it moves with the speed of social media. Given that reality, the court of public opinion is a more promising venue.

Governments should be expected to be part of the solution and not part of the problem. Instead of breaking into phones in a reckless manner, introducing huge risks, and producing little value, as discussed in Section 2.1.2, the government should make it a top priority to address confidence in all things digital. There are a number of government agencies with a mission to protect confidence in food, drugs, transportation, banking, etc. So too, there needs to be a regulatory agency with a mandate to address trust in all things digital.

Insurance policies[cj] have helped with confidence in banking. Credit cards are also protected by insurance.

Half of Americans had to have their credit cards replaced at least once because of internet fraud, including President Obama (Perlroth 2021, p. 268)

One could improve the security of credit cards, but credit card companies believe it is better to cover the losses than to discourage the use of their cards. So too, with spyware, there will come a time when governments and companies will introduce mechanisms to cover the losses so innocent victims are not left holding the bag. One could cover the cost of such an insurance policy by taxing all things digital or by imposing tariffs on countries that fail to take appropriate steps.

To file an insurance claim, victims could be required to admit that they have been hacked, and provide evidence to help investigators bring the criminals to justice. All too often, victims are reluctant to come forward. It was remarkable when the New York Times admitted to being hacked.[ck]

After Google, the New York Times was the first company to call the Chinese out directly for an attack on its systems. Just before I went to print with my story, my editors had done a gut check. Did we really want to publicize our attack? What would our competitors say? "Nothing," I told them. "They've all been hacked too." Sure enough, within hours of going to print, the Post and the Journal eagerly admitted that China had hacked them too. You weren't a credible news organization if you hadn't been hacked by China. The story opened the floodgates (Perlroth 2021, pp. 270–271)

6.2 Technical remedies

As suggested in Section 2.1.2, we should protect the keys to bank accounts by moving two-factor authentication back to a stand-alone fob that is kept in a safe with no connection to the Internet. The keys to our most important secrets should not be commingled with other stuff on our phones. There are a number of sensible principles in information security such as:

1. Minimizing attack surfaces
2. Compartmentalization

[ch] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

[ci] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[cj] https://www.fdic.gov/

[ck] https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

3. Defense in depth (DiD)
4. Audit trails

Audit trails could be useful as a deterrent. Now that disk storage is cheaper than bandwidth, it should be affordable to cache a few terabytes of Internet packet headers passing through wifi routers. There might be a technical solution for comparing caches across a few routers in a way that preserves privacy but makes it likely that hacks such as Pegasus will be discovered. The fact that such hacks tend to exfiltrate relatively large payloads should be useful for detection. These hacks will be easier to shut down if we can detect them more quickly.

There are surely more technical solutions to some of the problems mentioned above. Suppose that most of the components available on the market have been hacked by one government or another. Would it be possible, nevertheless, to come up with a trustworthy combination of untrustworthy components? That is, suppose there are two encryption boxes, B_a and B_b, where government G_a has a backdoor to B_a and government G_b has a backdoor to B_b. If we combined a few of these boxes in series, can we defend ourselves against both governments? Intuitively, it seems that there would be no defense against a government that has compromised an endpoint, but it is possible that there might be a solution where the attacker would need both backdoors. This problem is somewhat like RSA (Rivest *et al.* 1978), but in that case, one can unlock the secret with either key.

7. Conclusions

In previous work, we discussed Risks 1.0 (bias and fairness) and Risks 2.0 (addictive, dangerous, deadly, and insanely profitable). This work introduced Risks 3.0 (spyware). Risks 3.0 are less profitable, but more destructive.

On a positive note, Risks 3.0 have united forces that do not often unite. Journalists and tech companies are suing the same targets. This is something new, as mentioned at the end of Section 4.2.

Most of the discussion of these risks has more to say about problems than solutions. Progress will be made on Risks 3.0, but first, it will be necessary to raise awareness in the court of public opinion. After that, it will be much easier to make progress on technical and non-technical suggestions mentioned in Section 6. To get there, a number of of journalists are using the tools of their trade to raise awareness. We should do what we can to support them. This paper is a small step in that direction.

We would like to end with the following words of comfort from the poet Amanda Gorman, as spoken at President Biden's Inauguration, and quoted in the Pegasus book (Richard and Rigaud 2023, p. 97):

For there is always light,
if only we're brave enough to see it
If only we're brave enough to be it

References

Bergen M. (2022). *Like, Comment, Subscribe: Inside YouTube's Chaotic Rise to World Domination*. New York: Viking.

Church K., **Schoene A.**, **Ortega J. E.**, **Chandrasekar R. and Kordoni V.** (2022). Emerging trends: Unfair, biased, addictive, dangerous, deadly, and insanely profitable. *Natural Language Engineering* **29**, 483–508.

Fisher M. (2022). *The Chaos Machine: The Inside Story of How Social Media Rewired Our Minds and Our World*. New York: Little, Brown & Company.

Jeutner V. (2019). The Digital Geneva Convention: A critical appraisal of Microsoft's proposal. *Journal of International Humanitarian Legal Studies* **10**(1), 158–170.

https://doi.org/10.1017/S1351324923000141 Published online by Cambridge University Press

Koloßa S. (2019). Is there really a need for a new "Digital Geneva Convention"? Humanitäres Völkerrecht. *Journal of International Law of Peace and Armed Conflict* **1**(2), 37–52.

Li Y., **Yang X.**, **Sun P.**, **Qi H. and Lyu S.** (2020). *Celeb-DF: A large-scale challenging dataset for deepfake forensics*. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3207–3216.

O'Neil C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books.

Perlroth N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. New York: Bloomsbury Publishing.

Richard L. and Rigaud S. (2023). *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy*. New York: Henry Holt and Company.

Rivest R. L., **Shamir A. and Adleman L.** (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**(2), 120–126.

Thompson K. (1984). Reflections on trusting trust. *Communications of the ACM* **27**(8), 761–763.

Cite this article: Church KW and Chandrasekar R (2023). Emerging trends: Risks 3.0 and proliferation of spyware to 50,000 cell phones. *Natural Language Engineering* **29**, 824–841. https://doi.org/10.1017/S1351324923000141