Meet the Cybercriminals
Dr Victoria Baines
19 September 2023

Cybercriminals. Who are they? Are they really evil masterminds bent on world domination? Or are they awkward teenagers in gloomy bedrooms? Might they even be people like you and me? It depends on what we mean by 'cybercrime', and it depends on who is asking.

Is there a Cybercriminal Type?

One way to answer these questions is to look at criminal justice statistics. Ministry of Justice data for 2020 to 2022 tells us a certain amount about the demographics of defendants in criminal prosecutions in England and Wales.[1] The more technical cybercrime offences are categorised under the Computer Misuse Act 1990 as:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit further offences.
- Unauthorised acts with intent to impair.
- Making, supplying, or obtaining articles for use in said offences.

This covers most of what could be described as hacking and interference, but also writing and selling tools to help hackers. When we look at the data for these offences, we see that 85% of defendants are white, 88% are male, and by far the largest proportion (35%) are in their twenties. This seems to some extent to confirm the stereotype we see in movies, where hackers are very often portrayed as young white men. Unfortunately, criminal justice statistics tend not to record whether a defendant likes to wear hoodies.

Popular culture tends to associate technical ability with youth, to the extent that hackers in movies are often portrayed as boyish whiz kids, less mature and perhaps younger in years than other underground types. So, we may be surprised to find that under 18s represent just 3% of defendants for computer misuse.

But there are so many things this data doesn't tell us. It tells us nothing at all about the cybercriminals who don't get caught. It also tells us nothing about cybercriminals in other countries. According to the 2021 census, the population of the United Kingdom is 82% white.[2] While we don't have criminal justice data for other countries, media coverage of law

[1] https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2022
[2] https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/national-and-regional-populations/population-of-england-and-wales/latest

enforcement operations can be quite informative. In India, this is most often focused on Indian suspects, in Côte d'Ivoire on Ivorian suspects, and so forth. To some extent, this is inevitable, given that law enforcement agencies primarily have jurisdiction to pursue criminals within their national borders.

But as anyone who has ever been hacked will know, cybercrime is international, with offenders very often in a different country to their victims. This is particularly evident when cybercrime touches on national security issues. For example, the FBI's public Cyber Most Wanted list is much more ethnically diverse than our UK criminal justice data, partly because it includes individuals from Russia, Iran, China, and North Korea suspected of state-sponsored hacking.[3]

There are 119 individuals on the FBI's list at the time of writing (September 2023). Not a single one of them is identified as female. Women represent 12% of offenders in the criminal justice data set for England and Wales. How do we explain the complete absence of half the world's population from the ranks of global cyber outlaws?

It may be tempting to see this as confirming the erroneous belief of some that women are simply 'less technical' than men. Aside from the extent to which an assumption of technical (in)capability can exclude girls from education in STEM subjects, this explanation ignores several other possible influencing factors, among them an increased likelihood that state-sponsored cybercriminals work or have worked for the military and a hypothesis that links male dominance of cybercrime to increased prevalence of autism in males.

Recent research by cybersecurity firm Trend Micro found that around 30% of participants in underground cybercriminal fora are women.[4] Here they advertise their services and talk about their exploits, just as their male counterparts do. We'd need a lot of additional data in order to test this properly, but it does raise a number of intriguing questions. Are UK women less present in cybercriminal fora than the percentage reported by Trend Micro? It's possible, given that their research analysed a selection of English and Russian language fora. Or do women show up less frequently in criminal justice statistics because they're less likely to get caught? We shouldn't rule it out. In contrast to the biased assumption that women are 'less technical', it could in fact be the case that women are more successful cybercriminals in so far as they may be better at avoiding law enforcement attention. This in turn could be influenced by the fact that law enforcement isn't looking for them because they are not expecting to find them.

Women do write malicious software, as demonstrated by Trend Micro's research and the prosecution of Alla Witte for creating and deploying the Trickbot banking trojan and ransomware suite.[5] They are also active in the wider sphere of online crime – what law enforcement calls 'cyber-enabled' (as opposed to 'cyber-dependent') crime. Bulgarian national Ruja Ignatova, aka CryptoQueen, may not have made the FBI's Cyber Most Wanted list, but she is in its Top Ten of Most Wanted Fugitives for her alleged participation in the fraudulent OneCoin cryptocurrency scheme that resulted in investors around the world losing billions of dollars.[6] In July of this year, Heather Morgan, aka rapper Razzlekhan, pleaded guilty to money laundering and conspiracy to defraud the United States for her part in the hack of 4.5 billion U.S. dollars worth of Bitcoin from a cryptocurrency exchange.[7] In the cybercriminal ecosystem, the people who can dupe victims and turn data into hard cash are not bit players: they are central to the business model.

---

[3] https://www.fbi.gov/wanted/cyber
[4] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gender-in-cybercrime
[5] https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization
[6] https://www.fbi.gov/wanted/topten/ruja-ignatova/@@download.pdf
[7] https://www.bbc.co.uk/news/technology-66390639

What Motivates Cybercriminals?

The phrase ‘business model’ may suggest that all cybercrime is motivated by financial gain. But the motivations are several, not confined to a particular demographic, and not always distinct. We might assume that organised crime is driven by profit, governments and hacktivists by ideology, and teen hackers by the esteem and satisfaction that comes from beating a system designed to keep them out. It is not always that clear-cut. A court in the UK recently heard how two teenage boys diagnosed with autism were part of the Lapsus$ international cybercrime gang.[8] The elder of the two hacked BT and mobile operator EE, demanding a ransom of 4 million U.S. dollars on pain of deleting data. The boys also stole nearly £100,000 from a number of cryptocurrency accounts. While the prosecution cited “a juvenile desire to stick two fingers up to those they are attacking”, the prospect of financial gain was clearly also a factor.

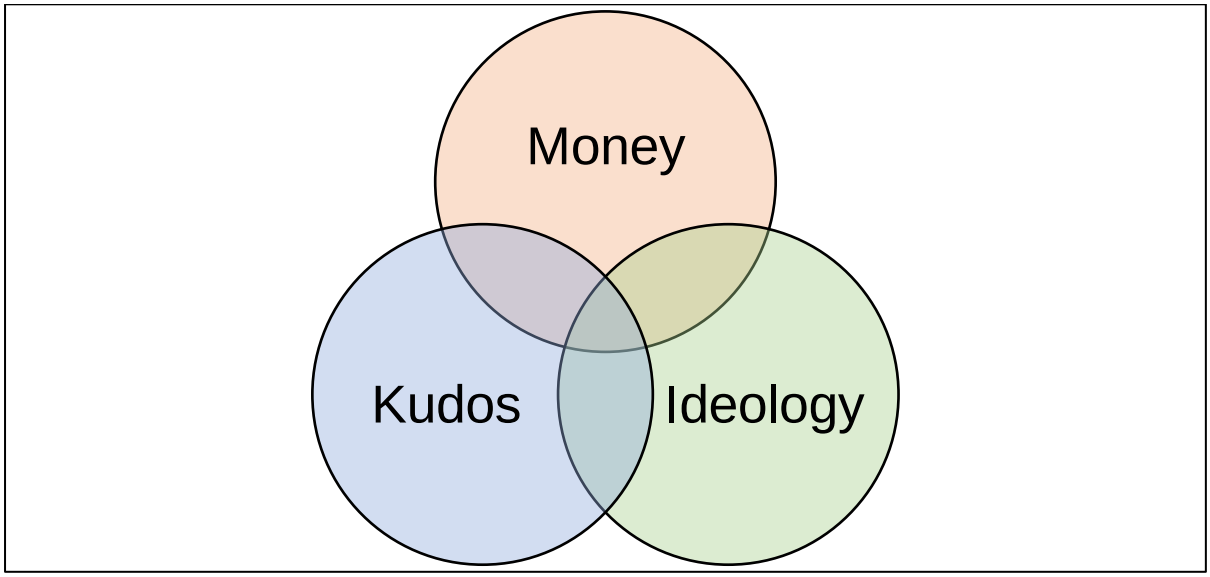

Fig. 1. Some motivations for cybercriminal activity.

We have also seen state-sponsored cybercriminals using ransomware, malicious software designed to extort money from victims. Far from having an ideological motivation, some countries have made cybercrime part of their government revenue generation. North Korea reportedly uses this business model to fund its espionage operations and nuclear proliferation.[9] The Bank of Korea in Seoul estimated that Pyongyang derived 8% of its GDP from cybercrime in 2020.[10]

Some types of cyber-enabled crime can also have surprising motivations. One would naturally expect the spread of fake news and disinformation to have political objectives. Government agencies wanting to influence the outcome of an election in another country or to sow discord in a society may be ideologically motivated. But the work of spreading false information is often outsourced to private companies and individuals whose motivation is financial. In one now-famous example, the Russian government reportedly paid young people in Macedonia to spread fake news during the 2016 U.S. presidential election campaign.[11] One young contractor said he was motivated by the prospect of buying trainers/sneakers and being able

[8] https://www.bbc.co.uk/news/technology-66549159
[9] https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage; https://foreignpolicy.com/2023/04/17/north-korea-nuclear-cyber-crime-hackers-weapons/;
[10] https://www.bloomberg.com/news/articles/2021-12-21/north-korean-army-of-cybercriminals-props-up-kim-s-nuclear-program-and-economy
[11] https://www.channel4.com/news/fake-news-in-macedonia-who-is-writing-the-stories

to afford a foreign holiday.[12]

People motivated by ideology to conduct cyber operations may not consider themselves to be criminals, even while they may actively engage in activity that disables digital services and interferes with communications. People from all over the world have joined the volunteer IT Army of Ukraine to engage in cyber operations against Russia. Its Telegram channel boasts a quarter of a million subscribers. A bilingual website provides attack instructions, suggested targets, command tools, and bots for distributed denial of service (DDoS) attacks aimed at disabling Russian government infrastructure. Several governments have warned their citizens against getting involved because there is no legal protection for civilians who conduct cyber-attacks, even if the cause is just.[13] Cybercrime is cybercrime is cybercrime.

Or is it? The schema in Figure 1 above presumes that people engage in cybercrime willingly, even if not always wittingly. But the last few years have seen the emergence of a new criminal business model in which people from as far afield as East Africa, the Middle East, and South America have been deceived into travelling to Southeast Asia, where they have been forced to work as online scammers. The United Nations has declared that it bears all the hallmarks of human trafficking: individuals are recruited and physically transported using coercion or deception to another location where they are exploited.[14] The UN estimates that 120,000 people in Myanmar and 100,00 in Cambodia are being made to work in this way. Are they cybercriminals or trafficking victims, or both? Should they be prosecuted or rescued?

In the first lecture of last year's series, *Who Owns the Internet?*, we discovered that different countries can have different definitions of what constitutes cybercrime. In the ongoing negotiations for a UN Cybercrime Treaty, several states have proposed that certain types of online speech be criminalised worldwide. Belarus, Burundi, China, Nicaragua, Russia, and Tajikistan want to outlaw "the distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions, or to provide access to such materials, by means of ICT". Egypt has called for the "spreading of strife, sedition, hatred or racism" to be criminalised, Jordan "hate speech or actions related to the insulting of religions or States using information networks or websites."[15] With such terms as 'enmity', 'strife', and 'insult' open to subjective interpretation, it's possible that many more of us will be branded as cybercriminals in the not-too-distant future, simply for expressing our political views or criticising someone in authority. Balances need to be struck carefully, between on the one hand minimising the use of IT to incite physical harm and, on the other, ensuring that our freedoms of speech and assembly are not unduly restricted.

So, are we all cybercriminals now? We clearly don't all commit technically sophisticated cybercrimes on a regular basis. But a considerable minority of us actively bend the rules and even break the law when using IT. A survey conducted by Forbes found that 42% of respondents used their work Virtual Private Network (VPN) to bypass geographical restrictions on streaming services.[16] Extensive sharing of passwords led to Netflix changing its policy in an effort to combat mass 'freeloading.'[17] In a 2021 survey, 1 in 8 European youths aged 16 to 19 reported engagement in money muling or laundering, 1 in 8 online harassment, 1 in 10 hate speech, hacking, and cyberbullying respectively, and 1 in 11 phishing, non-consensual

[12] https://www.france24.com/en/20180712-how-macedonian-town-became-fake-news-epicentre;
[13] https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
[14] https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf
[15] https://www.eff.org/deeplinks/2022/06/speech-related-offenses-should-be-excluded-proposed-un-cybercrime-treaty
[16] https://www.forbes.com/advisor/business/business-vpn-users-safety/
[17] https://about.netflix.com/en/news/an-update-on-sharing

sharing of intimate images, online fraud, and identity theft respectively.[18]

In my lecture *Cybersecurity for Humans*, we explored how cyber-attacks could be prevented through digital hygiene measures – the basic steps 'ordinary' (and not so ordinary) members of the public take could protect themselves, their friends and family, their businesses and their wider community. In *Defeating Digital Viruses*, we considered how the sheer scale of cybercrime, its international reach, and its pervasiveness in society make it suitable for a public health response with a focus on prevention at a population level, and targeted interventions for at-risk and affected groups.[19] In order to counteract cybercrime effectively, we therefore need to engage not only with potential victims but also with potential offenders. Some government agency programmes seek to raise awareness among young people of the distinction between legal and illegal online activity. Others seek to harness hackers' abilities and need for achievement for 'good', i.e., government-approved, activities. Both types of initiative depend on shepherding young people before they commit a crime that comes to the attention of law enforcement, to ensure that they follow the path of the White Hat rather than going over to the 'Dark Side'. As some of the cases above demonstrate, that line is not always so distinct. But once an individual has been convicted of an offence, it can prove legally and practically challenging to integrate them into the cybersecurity workforce.

Why Insight Matters

The cybercriminal population is diverse. It ranges from teenagers to the elderly, across all ethnicities, and even includes middle-aged women who are technically skilled (yes, really). Not all cybercriminals are stereotypical geeks. Not all are driven by a lust for profit, an extreme ideology, or devotion to a motherland. This matters for several reasons. A diverse population demands a range of prevention, disruption, and enforcement measures. Someone who is motivated by an extreme ideology may require deradicalisation to desist from offending, while someone who is driven into criminality by poverty may be better served by alternative employment opportunities.

A deeper appreciation of cybercriminals could also result in better enforcement.[20] The general assumption that cybercriminals are male may reflect male dominance in the cybersecurity industry and law enforcement cybercrime units, which in turn may lead to missed opportunities to profile suspects and defend against them effectively. We would need much more data to be able to test this hypothesis, but it would seem to make logical sense that the more representative the offender population in terms of gender, ethnicity, and neurodiversity, the better the insights and responses defenders can provide.

There is a significant practical challenge here, however. The more sophisticated cybercriminals are inevitably better at concealing their true identities, which means that they are often identified only in the later stages of an investigation. Some state-sponsored or APT ('Advanced Persistent Threat') groups operate for several years before any of their members are identified by name. Analysts and investigators therefore give them alternative names, sometimes based on a numerical system from 'APT 1' onwards, at others on a taxonomy of animal species and sub-species. The cybersecurity vendor Crowdstrike categorises its active cyber 'adversaries' as follows:

---

[18] https://www.ccdriver-h2020.com/_files/ugd/0ef83d_a8b9ac13e0cf4613bc8f150c56302282.pdf
[19] https://www.gresham.ac.uk/watch-now/digital-pandemic
[20] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gender-in-cybercrime

eCrime	Samba Spider	***China***
Punk Spider	Vice Spider	Vertigo Panda
Masked Spider	Bitwise Spider	Sunrise Panda
Squab Spider	Percussion Spider	Aquatic Panda
Merchant Spider	Solar Spider	Phantom Panda
Tunnel Spider	Sprite Spider	Lotus Panda
Hazard Spider	Traveling Spider	***Iran***
Honey Spider	Graceful Spider	Pulsar Kitten
Mangled Spider	Smoky Spider	Banished Kitten
Frozen Spider	Lunar Spider	Static Kitten
Odyssey Spider	Clockwork Spider	Charming Kitten
Chaotic Spider	Indrik Spider	***North Korea***
Royal Spider	Wizard Spider	Ricochet Chollima
Veto Spider	***Hacktivism***	Labyrinth Chollima
Wandering Spider	Frontline Jackal	Stardust Chollima
Recess Spider	Renegade Jackal	***Vietnam***
Brain Spider	***Russian Federation***	Ocean Buffalo
Holiday Spider	Gossamer Bear	***India***
Scattered Spider	Primitive Bear	Viceroy Tiger
Blind Spider	Cozy Bear	
Hermit Spider	Fancy Bear	
Alpha Spider	Voodoo Bear	
Aviator Spider	Venomous Bear	

Fig. 2. Selected state-sponsored, hacktivist, and profit-driven cybercriminal groups, reproduced from Crowdstrike's 2023 Global Threat Landscape (see Further Reading*).*

To take just a couple of examples from the table above, North Korean group Stardust Chollima is also known as APT38 and Hidden Cobra, and more popularly as the Lazarus Group, some of whose alleged members are identified in the FBI's list of Cyber's Most Wanted. Active since at least 2009, Lazarus is believed to be behind the hack of Sony Pictures in 2014, the theft in 2016 of close to 1 billion U.S. dollars from the central bank of Bangladesh, and the 2017 WannaCry global ransomware attacks.

Russian group Fancy Bear is also variously known as APT28, Pawn Storm, Sofacy Group, Sednit, Tsar Team, and STRONTIUM. This group's targets have reportedly included European governments, political opponents of the Russian government, French television station TV5Monde, the World Anti-Doping Agency, the U.S. Democratic National Committee, and the Ukrainian military.

While these naming systems came about as a practical workaround, a means to refer to cybercriminals prior to their identification as individuals, they have arguably contributed to mythologising these groups. They mystify our appreciation of them, transforming them into abstract concepts or fantastic beasts, and preventing us from getting the measure of them as humans. This kind of treatment bestows on sophisticated cyber actors precisely the kind of kudos many of them seek – unless, of course, they are unfortunate enough to be in the group known as Charming Kitten.

There is growing concern about the misuse of Artificial Intelligence for cybercrime. Cyber-attacks are increasingly automated, and it's already possible for criminals to use publicly available tools such as ChatGPT to write scam marketing materials and phishing emails. Recognised potential for self-learning malware and the prospect of further advances raises the possibility of machines as bad actors, cybercriminals in their own right. But for the time being at least, there is still a person behind every cybercrime. Understanding their thoroughly human impulses is challenging but necessary and – in my opinion – utterly fascinating.

Further Reading & Resources

You can read more about the activities of sophisticated cybercriminal groups in the publications of cybersecurity providers, including:

Crowdstrike (2023) *Global Threat Landscape*. https://www.crowdstrike.com/adversaries/

Mandiant (2023) *M-Trends Report*. https://www.mandiant.com/m-trends

Trend Micro (2023) *2023 Midyear Cybersecurity Threat Report*. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report

A number of popular books, audiobooks, and podcasts detail how cybercriminal groups operate and the lives of some notorious personalities. The following are recommended:

Jamie Bartlett (2021) *The Missing Cryptoqueen*. WH Allen. Also as a BBC podcast - https://www.bbc.co.uk/sounds/brand/p07nkd84

Misha Glenny (2011) *DarkMarket: How Hackers Became the New Mafia*. Vintage.

Geoff White (2022) *The Lazarus Heist: From Hollywood to High Finance: Inside North Korea's Global Cyber War*. Penguin Business. Also, as a BBC podcast - https://www.bbc.co.uk/sounds/brand/w13xtvg9

The following on the demographic profiles of cybercriminals is available on Open Access:

Ciaran Jenkins (2016) "Fake online news from Macedonia: who's behind it?", *Channel 4 News* 24.11.2016 https://www.channel4.com/news/fake-news-in-macedonia-who-is-writing-the-stories

CNN (2017) *The Fake News Machine: Inside a town gearing up for 2020*. https://money.cnn.com/interactive/media/the-macedonia-story/

Mayra Rosario Fuentes (2023) *The Gender-Equal Cybercriminal Underground*, Trend Micro - https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gender-in-cybercrime

Katy-Louise Payne, Ailsa Russell, Richard Mills, Katie Maras, Dheeraj Rai, and Mark Brosnan (2019) "Is There a Relationship Between Cyber-Dependent Crime, Autistic-Like Traits and Autism?", *Journal of Autism and Developmental Disorders* 49(10): 4159–4169. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6751221/

Samanth Subramanian, "Inside the Macedonian Fake News Complex", *Wired* 15.02.17. https://www.wired.com/2017/02/veles-macedonia-fake-news/

A more detailed discussion of the legal and ethical issues of hacking for a good cause can be found in my January 2023 piece for *Wired* magazine, "Hacktivism is a risky career path". https://www.wired.com/story/cybersecurity-hacktivism/

Among the resources aimed at diverting young people from a cybercriminal career path is the UK National Crime Agency's Cyber Choices initiative: https://www.nationalcrimeagency.gov.uk/cyber-choices