How to catch a crook: behind the scenes of a police raid on a cyber-criminal's home

Faceless, nameless cyber-villains are notoriously hard to catch. Carl Miller joins the police on an operation that brought one blinking into the daylight — and to justice

GETTY IMAGES

The Sunday Times, August 19 2018, 12:01am

'This is the third phase of Operation Field-Day," says the police officer. A photo of the suspect is silently passed around. He's in his thirties, but looks many years younger. "His arrest is necessary to protect vulnerable persons and property," the officer continues, as I stare at the man in the picture. A thin beard, short downy hair, unblemished skin and, at a glance, soft, even kind, eyes.

A sweltering July day was beginning to draw into dusk. I was in a building in the middle of a featureless industrial park. Neatly trimmed bushes, empty pavements, glass and brick; it could have been anywhere. But if you tapped one of the "rotting" wooden bollards that surround the building, you'd notice a difference — they are actually metal, and would probably stop a tank.

The front door of the building was blastproof. Inside, framed portraits — one after the other — neatly lined the wall. An Uzi sub-machinegun. A yacht. Thirty bin bags full of drugs. A fleet of Range Rovers. Photographs of goods seized from criminals. I was in a covert police headquarters.

The light now fading, we pulled out of the building in a small convoy. Three unmarked police cars quietly snaked through evening traffic, past emptying parks and filling restaurants. A radio squawked from the boot, but otherwise the car was silent. The sergeant turned to me: “It’s going to be an uncomfortable situation. There’s a wife and a child there. They’re going to wonder what he’s done.”

One morning in 2015, Susan, a 28-year-old woman from the east of England, woke up and discovered she couldn’t log on to her Facebook or Twitter accounts. She couldn’t control them because somebody else was. They were sharing a stream of photographs to all her contacts, including her family, friends and colleagues. Horrified, she watched as image after image appeared. They were all sexually explicit, private pictures of her. Susan had been the victim of a horrific, violating, misogynistic kind of robbery while she slept. Her Twitter and Facebook accounts had been stolen, but also her Apple iCloud account, and with it every picture, every text, every call, every WhatsApp message that had passed through her iPhone. She complained to the police, but nothing happened. There wasn’t much, she was told, that they could do.

Eventually, the images stopped. But then, in 2016, the nightmare recurred. Again, her iCloud account was seized. Again, sexual images of her were shared on the internet, but this time even more widely. She found herself on shaming sites, amateur porn sites, often with her full name and contact details. She was flooded with calls and messages from nameless, faceless men all over the world, propositioning her, offering to help or simply gloating.

Susan went to the police again for help, and this time the report reached Brandon, a detective constable in the local force. He went from lead to lead, following a meandering online trail. Sometimes the trail vanished, sometimes it led him into dead ends, but eventually it brought him to a small website dedicated to the sharing of amateur sexual images. “It’s a British community. It’s all UK,” Brandon explained. “It’s all about people looking for images of women living close to them — women that they might know. That’s their thrill.”

Behind the public face of the website, Brandon found a hidden area — an inner circle of 3,000 users who had paid money or shared images for access. This was where special “wins”, as they called them, were shared. Here, naked images of women were used as a currency, especially those not seen before and not in public circulation. It was a flourishing community of people working with each other to steal iCloud accounts. Eventually, Brandon managed to piece together the identities of some of those on the forum, and that trail led us to the suspect that we were now heading to confront.

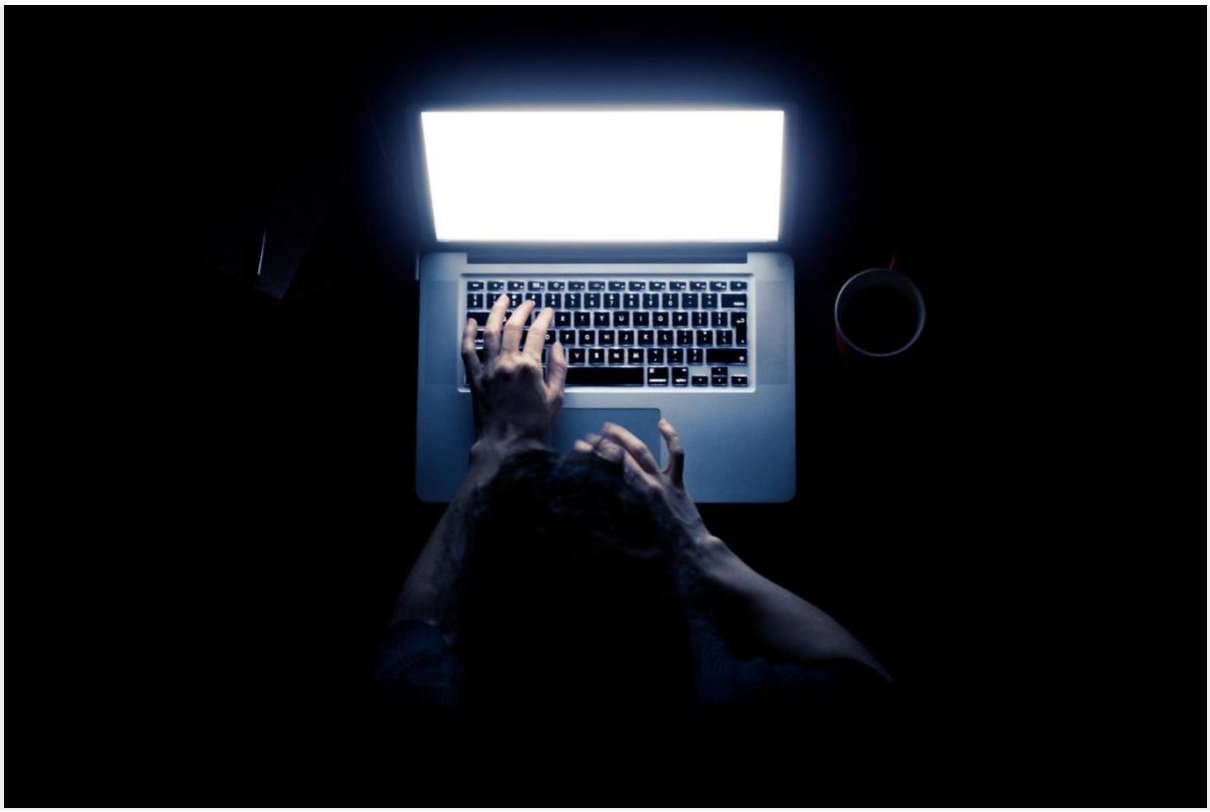
It was evening by the time the convoy pulled up to our destination. With the car idling, the officers scanned a large red-bricked house with a white stucco front. It was in the middle of a new suburban estate; an affluent, claustrophobic commuter dormitory. Neatly planted flowerbeds ringed the outside of the house, and the curtains of the neighbours had started twitching.

We sat in tense silence, watching the house, looking for movement. “OK,” the sergeant said. “Let’s go.” He and Brandon knocked on the door, it opened and they disappeared into the house. Minutes ticked by until, finally, the silence was broken. Above the hiss of radio, I heard that it had been the suspect’s wife at the door. He wasn’t home. Away at a conference, he was expected back later that evening.

Upstairs was the cyber-criminal’s lair, a comfortable, domestic computer room. There were Iron Man and Thor posters on the wall, next to Captain America’s shield. The couple’s marriage certificate was perched on top of a stack of paper, and two doors down from the computer room, their child was quietly sleeping. But among the domesticity, the police became more and more suspicious. The suspect had a large box crammed with Sim cards for different mobile phones and about a dozen hard drives pushed into a corner. “A normal person just doesn’t have all this stuff,” one of the officers muttered as she crammed bag after bag with carefully catalogued evidence.

Then, there was a ripple of motion. The man’s car had pulled up outside the house. The door opened and the suspect stepped in. Worried scenarios ran through my head. What if something went wrong? What if the suspect pulled a knife?

In the flesh, he looked even younger than his photograph, pale and blinking hard in disbelief at the police officers standing in front of him. I'd read the private messages he'd sent on the forum — his obsession with the "win", the naked photos, the advice he'd offer to new members, allusions he'd made to a mysterious collection he'd been archiving and cataloguing, and all the discussions he'd had about how to avoid getting caught by the police. But as Brandon stepped forward to arrest him, all of that chatroom bravado drained away. The suspect's prominent Adam's apple kept wobbling as he vainly tried to swallow. He was so shocked, he could barely talk. He could barely even stand. Supported by the officers as much as led by them, he went out to their car without uttering a word. There was no resistance whatsoever.



You are 20 times more likely to be robbed at your computer than mugged in the street ALAMY

He was the most unhardened criminal I'd ever seen, and that shouldn't have been a surprise. Online offenders were, I was told, often like this suspect— shy, stammering and awkward. "You can't just profile the rough kids living on the council estate now as the ones that will turn to a life of crime. It isn't like that any more," the police had told me. "They're often kids that don't venture outside of the house. They're stuck in their room. You can be a different person online than you are in the real world. And no one else can see that."

Yet he had begun to feel a kind of control that he'd never had before. He could invade people's intimate lives without them even knowing. It wasn't only new kinds of crimes being committed. It was also new kinds of criminals committing them, drawn to dark new routes to power.

It was early in the morning by the time we returned from the raid. Lightning rolled across the sky, and rain silently tumbled onto the thick, blastproof windows of the covert police station.

Under harsh white neon light, the police officers sipped coffee and started eating a mound of chips. I watched as they began to seize each of the suspect's online identities: his email addresses, his social media accounts, his messaging apps. Message after message, file after file, they began to build a picture of the suspect's secret life, as intimate and detailed as the files he had stolen from his victims.

It wasn't surprising that this cyber-criminal existed, nor his thousands of friends within that closed forum. More than 40% of the crimes that people living in the UK experience are committed through the internet. Online fraud has become our most common crime. You are 20 times more likely to be robbed at your computer than mugged in the street. Your social media accounts are as likely to be burgled as your house. Operation Field-Day was part of something much bigger — we have lived through a staggering change in how and where crime happens.

Some of what the suspect had done was sophisticated, intricate and incredibly hard to trace, and that shouldn't have been a surprise either. Because while the barriers to entry to cyber-crime are incredibly low, its most advanced forms soar beyond what most of us can imagine.

There was, I realised then, only one thing about Operation Field-Day that really did set it apart — that it existed at all. The suspect had been caught largely because he had been unlucky. "Almost every single investigation," an officer told me, "hits the same basic wall. You can't reach the victims. You can't reach suspects. When it leaves the UK, we can't get involved. We can't chase them. It doesn't matter if they're in China, Russia or Germany, we can't do anything about it, at our level."

A scam, a piece of malware, an extortion, child-abuse images — they all flash across the world in an instant. A person in Cambridge has their life savings stolen and the trail disappears into Russia. Investigation over.

A criminal's phone is seized in Essex and there are indications that a scam has targeted people in India. Investigation over. Victims, suspects and the evidence that linked them together are scattered all over the world. Crime on the internet — like anything on the internet — flows across borders with incredible ease. But one thing that doesn't is law enforcement.

"If they use any service, any server based outside the UK, you're in trouble," I was told. If the trail of digital evidence leads to a co-operative jurisdiction, it can be time-consuming and expensive to get the information. Police investigations, however, often lead to jurisdictions that won't co-operate, and then there is almost nothing the police can do about it. "People from non-cooperative jurisdictions can pretty much act with impunity," one officer said. "It's incredibly frustrating for us. Until we sort out international policing, the risk of committing cyber-crime is basically nil."

"Unless we start moving at pace, it could become a crisis," Stephen Kavanagh told me. Stephen is chief constable of Essex police, the chair of the digital policing board at the National Police Chiefs' Council and the national policing lead on digital investigations and intelligence.

"This is the most profound shift the police have experienced since Peel [the father of modern policing]," he continued. "We will adapt in a way more fundamental than anything since Peel's reforms. But we, the police, can't do it alone. Based on the scale of cyber-crime that we've now seen, I can't be optimistic until I see us working across government departments. This is not just a law-enforcement problem, this is a social problem.

"What we are seeing," he said, "is that victims and others are turning to other bodies to deal with their concerns." What is at stake here is the basic relevance of police to cyber-crime at all.

At the moment when crime began to migrate online, everyone thought crime figures were falling. In 2014, before the scale of cyber-crime was known, Theresa May, in her role as home secretary, declared: "Police reform is working and crime is falling . . . We have achieved something no modern government has achieved before. We have proved that, through reform, it is possible to do more with less." Overall, funding for police dropped by about a fifth between 2011 and 2016; in 2016, there were 21,000 fewer police officers than in 2010.

But crime wasn't falling, it was simply transferring into new forms we've only just begun to count. "The bandwidth does not exist," Stephen told me. "My force is still trying to find savings after eight years of austerity. The infrastructure that underpins the transformation is missing."

So the period when the police force needed to begin to reshape itself to respond to cyber-crime was exactly the time when its budget was being cut. Indeed, it appears some police forces are actually decreasing spending on digital infrastructure.

I came away from my time with the police depressed and worried. For all the amazing benefits digital technologies have brought us, there is one terrible downside — crime is benefiting far more from these developments than law enforcement. The means by which people can reach in and shape our lives — and us theirs — have changed in breathtakingly radical ways. But as all our lives become more digital, the law itself — the politicians who pass it, the judges who interpret it and the police who enforce it — becomes less relevant. The organisations that were most responsible for controlling power are exactly those that have been made most powerless by the digital revolution.

This is a crisis of law enforcement. It has already happened, and it will only get worse. And between the police and the criminals are all the people the law is supposed to protect.

People like Susan who have watched, powerless, as their accounts have been hijacked and used against them; millions of people who are being defrauded, hacked, extorted and invaded online. As criminals become more powerful, it is their victims that really become more powerless.

It was some months later that the first of the Operation Field-Day trials went ahead. It was a great victory for the operation and for Brandon — a conviction and a heavy custodial sentence. Brandon himself was nominated for an award for the skills in digital investigation that he'd brought to this case and to others. That was, of course, entirely the problem: Brandon is an exception, not the rule, in policing, and so was Operation Field-Day. This wasn't, I knew, how most stories about cyber-crime end.

Masked intruders: thousands of hackers converge on the annual Def Con conference to share new ways of exploiting weaknesses in technology, from mobile phones to wind turbines GENE BLEVINS/POLARIS

“He controlled a laptop using only light”
At an annual gathering of top hackers in Las Vegas, the terrifying extent of our vulnerability is laid bare

Half a world away, the vast neoclassical edifice of Caesars Palace sits right in the middle of the Las Vegas strip. Inside, it is all pink and white marble; glitz and vice. Outside, women in bikinis and men in shorts play in the fountains and pick at food from Snackus Maximus. But, once a year, a new kind of player arrives in town. Black jeans, black T-shirts, pirate bandannas, neon-blue mohawks, Japanese anime tattoos. Some wear full-face masks, others steampunk goggles. For a few days in summer every year, Las Vegas becomes the site of the most important annual gathering of hackers in the world: Def Con.

On Def Con’s biggest stages, the year’s most cunning and sensational hacks are revealed. To the whoops and cheers of 10,000 assembled hackers, each was an example of arcane and technical mastery.

I watched as a hacker, in dull monotone, showed the audience how he could control a laptop simply using light. Then light you couldn't see. Then sound. Then sound you couldn't hear. I watched hackers show how they could seize control of the turbines of wind farms and cause one to stop-start-stop-start-stop-start until it would shudder to the ground or burst into flames. One hacker group called the Exploiteers seized control of cameras, printers, routers and doorbells. Another — a shadowy Chinese group — could receive calls meant for your mobile phone, and send calls as if you'd made them. I watched hackers turn an innocent computer mouse into an attack vector by injecting their own code into its microprocessor. And others hack voting machines to change the records of who had voted for whom.

These hackers sit on both sides of the law. And fight across many of the political and social struggles that now take place, in part, online. There are neo-Nazi hackers, anarchist hackers, hippie hackers. But reality has become a sort of playground for those with enough talent, skill and, in many cases, bloody-minded obsession to make the technology woven through our daily lives answer their commands.

Power: a new world order

The inability to police cyber-crime is part of a trend that sees old hierarchies being overturned by the digital revolution

The old gods are dying. Shops are collapsing along the high street. Stock prices plummet with a tweet. Newspapers are being swallowed. Governments are losing control. The authorities are struggling to police cyber-space. The old familiarities have come tumbling down and new social orders, new hierarchies, new winners have started to emerge that all, in one way or another, trace back to digital technology. Facebook has grown bigger than any state, bots battle elections, technologists have reinvented democracy and information wars are breaking out around us.

Amid all this change, I was afraid that we were hurtling into a new social reality that we didn't really understand and couldn't anticipate. Yet for centuries there has been a single idea that we've always turned to during moments of seismic change. Machiavelli, Hobbes, Marx, Foucault had all used it to understand their own changing worlds. It is power, that capacity we all hold to shape, in different ways, the lives of those around us — and others to shape ours.

Now, I decided, is again the time to expose the reality of power. To ask the deeper questions about how our lives are shaped. Whether we are more powerful as individuals than ever before, or more controlled. And whether technology is propelling us towards a new dawn of liberation, or a nightmare of subjection.

As it has in the past, this slippery yet important idea was what we needed to stop sleepwalking through a revolution.

So I went on a strange, uplifting and, on occasion, personally terrifying journey in pursuit of power. It took me through freezing courtyards in Berlin to neon-drenched Seoul, inside a busy army base in Berkshire, to a colourful jamboree in Mexico, and across the sprawling campuses of Silicon Valley.

I lived in a political-technology commune in east London, peered into the mechanics of secret algorithms, became involved in a struggle for control of an online assassination market and even tried to hack a hacker. I spoke to presidents and digital ministers, spies, soldiers, criminals, guerrilla viral artists, hackers, a fake-news merchant and a tech whistleblower.

Some were newly powerful, others newly powerless. But all of them became my guides and interpreters to forms of power that were quickly on the move.

Everywhere I looked, I found power escaping from its old bonds. Whether it was across politics or crime, in warfare, the media or technology itself, and even within each of us, power was being fought over and transformed. It was touching our lives in weird new ways we could scarcely imagine. As the old gods die, new gods are being born, and we are only beginning to comprehend the world they are making.

Some names have been changed.

@carljackmiller